



Web Filtering and Reporting Suite
Evaluation Guide

Models: 350, 550

Version 5.1.00

Publication Date: 29 April 2013

Legal Notice

Copyright © 2013 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained from:

www.trustwave.com/support/

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Part# WFR-IG-130429

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.




Format and Symbols	Meaning
<u>Blue Underline</u>	A blue underline indicates a Web site or email address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
Code	Text in this format indicates computer code or information at a command line.
<i>Italics</i>	Italics are used to denote the name of a published work, the current document, or another document; for text emphasis; or to introduce a new term. In code examples italics indicate a placeholder for values and expressions.
[Square brackets]	In code examples, square brackets indicate optional sections or entries.
	Note: This symbol indicates information that applies to the task at hand.
	Tip: This symbol denotes a suggestion for a better or more productive way to use the product.
	Caution: This symbol highlights a warning against using the product in an unintended manner.

Table of Contents

Legal Notice	ii
Formatting Conventions	iii
List of Figures	ix
List of Tables	xi
1 WFR Evaluation Guide	13
1.1 Market Overview	13
1.2 Product Overview	13
1.3 Note to Evaluators	14
1.4 Install the WFR	14
1.4.1 Operating systems and browser types supported	14
1.4.1.1 Administrator Workstation Requirements	14
1.4.1.2 End User Workstation Requirements	15
1.4.1.3 Ports used on the network for a secure connection	15
1.4.2 Use the single-sign on option	16
1.4.2.1 Default usernames and passwords for WFR applications	16
1.5 Database Initialization	16
2 Web Filter Evaluation	17
2.1 Configure and Test the Web Filter	17
2.1.1 Understand the most common and useful features	17
2.1.2 Update Libraries	17
2.1.3 Group setup for different user types on the network	17
2.1.3.1 Apply different filtering levels for different types of users	17
2.1.3.2 Rules and Profiles: Creating and using each	19
2.1.3.3 Global Group Profile	22
2.1.3.4 Group Profile	23
2.1.4 Group settings tests	24
2.1.4.1 Test the Rules and Profiles feature	24
2.1.4.2 Test the Rule	25
2.1.5 Custom Categories	26
2.1.5.1 Create and configure a Custom Category	26
2.1.6 Filtering profile features	28
2.1.6.1 Time Profile feature	28
2.1.6.2 Quota feature	29
2.1.6.3 White List feature	31
2.1.6.4 Warn feature	32

2.1.6.5 Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement	33
2.1.6.6 Search Engine Keyword Filtering	34
2.1.6.7 Attachment filtering	36
2.1.6.8 Wildcard filtering	37
2.1.7 Configure, test, block services	39
2.1.7.1 Anonymous proxies	39
2.1.7.2 Block IM, P2P applications and streaming media	40
2.1.8 Real Time Probes and X-Strikes Blocking	42
2.1.8.1 Real Time Probes feature	42
2.1.8.2 X-Strikes feature	43
3 Security Reporter Evaluation	49
<hr/>	
3.1 Configure and Test Productivity Reports	49
3.1.1 Understand the most common and useful features	49
3.1.2 Use Custom Category Groups to narrow your search.	49
3.1.2.1 How to add a Custom Category Group	50
3.1.3 Use custom User Groups to narrow your search	50
3.1.3.1 How to create User Groups	51
3.1.3.2 How to Rebuild a User Group	54
3.1.4 Use Security Reporter to conduct an investigation	54
3.1.5 Use Summary Reports for a high level overview	56
3.1.5.1 How to generate a Summary Report	56
3.1.5.2 How to export a Summary Report	59
3.1.6 Use Drill Down Reports for an investigation	59
3.1.6.1 How to generate a Summary Drill Down Report	60
3.1.6.2 Summary Drill Down Report navigation	60
3.1.6.3 How to generate a Detail Drill Down Report	62
3.1.7 Create a custom report for a specific user	65
3.1.7.1 How to use the Report Wizard for a single user report	65
3.1.8 Export Summary Drill Down Reports	70
3.1.8.1 How to export selected records	70
3.1.8.2 Sample report file formats.	72
3.1.9 Summary Drill Down Reporting tools	73
3.1.9.1 How to use other Summary Drill Down Report tools.	73
3.1.10 Commonly used reports	77
3.1.10.1 How to generate a Sample Report	77
3.2 Configure and Test Real Time Reports	80
3.2.1 Understand the most common and useful features	80
3.2.2 Monitor URL gauges	80
3.2.2.1 How to drill down into a URL gauge	81
3.2.2.2 How to view URL Trend Reports	85
3.2.2.3 How to view a pie chart for a URL gauge	87
3.2.3 Monitor Bandwidth gauges	88
3.2.3.1 How to view the Bandwidth gauges Dashboard	88

3.2.3.2	How to drill down into a Bandwidth gauge	89
3.2.3.3	How to view Bandwidth Trend Chart activity	92
3.2.3.4	How to view charts for a specific Bandwidth gauge	93
3.2.4	Get the complete picture	94
3.2.4.1	How to view Overall Ranking of user activity	94
3.2.4.2	How to create a New Gauge	95
3.2.4.3	How to create an automated gauge alert	99

List of Figures

Figure 1:	The main Policy screen	18
Figure 2:	IP Group members	19
Figure 3:	Profile window, Rule tab	20
Figure 4:	Rules window	21
Figure 5:	Global group profile, Category tab	22
Figure 6:	Group Profile window, Category Profile tab	23
Figure 7:	Rules window	24
Figure 8:	IP group profile window with rule applied	25
Figure 9:	Custom Categories in Library tree menu	26
Figure 10:	Block page	27
Figure 11:	Time Profile window	28
Figure 12:	Adding Time Profile window	29
Figure 13:	Quota time shown in Quota column and Overall Quota enabled	30
Figure 14:	Quota Setting window	31
Figure 15:	White list rule setup	32
Figure 16:	Safe Search Enforcement Filter Options	33
Figure 17:	Search Engine Keyword filtering	34
Figure 18:	Adding Search Engine Keywords	35
Figure 19:	Attachment filtering setup in URL Keywords	36
Figure 20:	Attachment filtering setup in Filter Options tab	37
Figure 21:	Wildcard filtering	38
Figure 22:	Block anonymous proxies	39
Figure 23:	Block patterns	41
Figure 24:	Real Time Probe setup	42
Figure 25:	X-Strikes feature	44
Figure 26:	X Strikes Blocking	45
Figure 27:	X Strikes testing	47
Figure 28:	Custom Category Groups panel	50
Figure 29:	User Groups panel	51
Figure 30:	New User Group panel	52
Figure 31:	Add user group, IP Ranges sub-panel	53
Figure 32:	Add user group, Single Users sub-panel	54
Figure 33:	Yesterday's Top 20 Users by Blocked Requests Report	57
Figure 34:	Sample Bar Chart Summary Report in the PDF format	58
Figure 35:	Sample Pie Chart Summary Report in the PDF format	58
Figure 36:	Sample Drill Down Categories Report (summary report)	60
Figure 37:	Detail Drill Down Report view	63
Figure 38:	Report Wizard panel for summary reports	66
Figure 39:	Report Wizard panel for detail reports	66
Figure 40:	Drill Down Report Wizard's Save Report panel Basic Options tab	68
Figure 41:	Drill Down Report Wizard's Schedule Report panel	69
Figure 42:	Saved Reports panel	70
Figure 43:	Category Groups report, PDF format	73
Figure 44:	Sample Category/Users report	79
Figure 45:	Sample User/Sites report	79
Figure 46:	Sample Category/User/Sites report	80
Figure 47:	URL dashboard with URL gauges	81
Figure 48:	Gauge Ranking panel	83
Figure 49:	List of Threats accessed by the user for a gauge	83
Figure 50:	List of URLs for the selected threat	84
Figure 51:	User Summary panel	85
Figure 52:	URL Trend Charts panel	86
Figure 53:	Activity for a specified gauge	87
Figure 54:	Gauge Trend Chart	88
Figure 55:	Bandwidth gauges Dashboard	89
Figure 56:	Bandwidth used by each end user for a protocol	90
Figure 57:	User Summary panel showing the user's bandwidth protocol usage	91
Figure 58:	Category View User panel showing the user's port usage	91
Figure 59:	Bandwidth Trend Charts panel	92

Figure 60: Line chart for a bandwidth gauge. 93
Figure 61: Bandwidth Gauge Trend Chart for a specified protocol (HTTP). 93
Figure 62: Line chart for a specified port. 94
Figure 63: Overall Ranking table 95
Figure 64: Add/Edit Gauges panel 96
Figure 65: URL Gauge panel 97
Figure 66: Sample Alerts panel with URL Gauges tab selected. 99
Figure 67: Sample Bandwidth Gauges panel, email criteria 102

List of Tables

Table 1:	Administrator workstation requirements	14
Table 2:	End user workstation requirements.	15
Table 3:	Application interface ports	15
Table 4:	Application default credentials	16

1 WFR Evaluation Guide

1.1 Market Overview

In order to survive in today's world, businesses continually come up with new products, more sales, and better service. But most often, the corporate world is financially threatened from the inside. Employees harm businesses when they view pornography and other offensive Web content at work, which often result in sexual and hostile work environment lawsuits. Organizations also lose time and money when employees tie up network bandwidth with IM and P2P, and/or allow spyware and malware into the system. And finally, a host of federal and state laws require that organizations protect customer data, or risk severe penalties.

Trustwave's Web Filtering and Reporting Suite (WFR) not only helps companies maintain compliance with laws such as the California Security Breach Information Act (CSBIA), but also helps protect the security of a company's network infrastructure. With no premiums, ease of installation and usage, and 24-7 technical support, Trustwave's WFR is the perfect choice for overburdened IT administrators and managers.

1.2 Product Overview

The Trustwave WFR, comprised of the Trustwave Web Filter and Trustwave Security Reporter, is designed to complement existing security measures by providing protection from threats *inside* the network—the threats most often unseen and discovered too late.

The Web Filter tracks end users' online activity and can be configured to block specific Web sites or service ports, thereby protecting organizations against lost productivity, constricted bandwidth and possible legal liability resulting from Internet content. This product also features expansive content categories (called libraries), instant message and peer-to-peer blocking, user authentication, and intuitive administrative navigation. All of these features are provided in a true appliance that provides speed and stability unmatched by any software product. In addition, the Web Filter is fail-safe giving administrators the peace of mind that filtering won't ever impact the network's performance—or shut it down.

The Security Reporter helps administrators manage internal Web-based threats by documenting historical Internet usage information by user. Built on a dedicated MySQL server database that works in conjunction with the Web Filter, the SR handles substantial amounts of Internet traffic because of its unique processing approach, which pre-processes and indexes data in a format conducive to high-speed retrieval without compromising filtering performance or impacting network functions. The SR utilizes filtering logs to help administrators monitor Internet usage information by user *in real time*, and by providing proactive remediation tools to enforce the organization's Acceptable Use Policy.



Note: Although a Trustwave Secure Web Gateway (SWG) can be connected to the WFR to send logs to its Security Reporter application, this Evaluation Guide will only focus on using the WFR's built in Web Filter to send logs to the Security Reporter. For information on using an SWG with the Security Reporter, please see the Trustwave Security Reporter Evaluation Guide for software version 3.2.0.

1.3 Note to Evaluators

Thank you for taking the time to review Trustwave's WFR. Your interest in our company and product is greatly appreciated.

The exercises in this document are presented to you in a very explicit way and easy-to-follow manner so that you may quickly become comfortable with the user interfaces of each application.



Caution: Disable Pop-up Blocking Software: Please note that a user with pop-up blocking software installed on his/her workstation will need to disable pop-up blocking in order to use this application.

1.4 Install the WFR

To install the appliance and configure basic settings, please refer to the step-by-step instructions found in the **Trustwave Web Filter and Reporter Installation Guide** provided in the shipping carton.

After the appliance is set up on your network and configured using one of the methods described in the Installation Guide, proceed to the Web Filter and Security Reporter sections of this Evaluation Guide to review the user interfaces for each application in this product.

1.4.1 Operating systems and browser types supported

1.4.1.1 Administrator Workstation Requirements

System requirements for the administrator include the following:

Table 1: Administrator workstation requirements

Client OS	IE version	Firefox version	Chrome version	Safari version
Windows XP	8	16	23	N/A
Windows Vista	9	16	23	N/A
Windows 7	9	16	23	N/A
Macintosh 10.6 (Snow Leopard)	N/A	17	23	5
Macintosh 10.7 (Lion)	N/A	17	23	6
Macintosh 10.8 (Mountain Lion)	N/A	16	N/A	6

- JavaScript enabled
- Java Virtual Machine
- Java Plug-in
- Pop-up blocking software, if installed, must be disabled

- Session cookies from the WFR server must be allowed in order for the Administrator consoles to function properly

1.4.1.2 End User Workstation Requirements

System requirements for the end user include the following:

Table 2: End user workstation requirements

Client OS	IE version	Firefox version	Chrome version	Safari version
Windows XP	8	16	23	N/A
Windows Vista	9	16	23	N/A
Windows 7	9	16	23	N/A
Macintosh 10.6 (Snow Leopard)	N/A	17	23	5
Macintosh 10.7 (Lion)	N/A	17	23	6
Macintosh 10.8 (Mountain Lion)	N/A	16	23	6

- JavaScript enabled
- Pop-up blocking software, if installed, must be disabled

1.4.1.2.1 Supported Tablets

The following tablets are supported—with a few exceptions to some features, as denoted in the WFR Administrator Guide: iPad1 (iOS 5.5), iPad2 (iOS 6), Galaxy Tab 7.0 (Android 2.2, Froyo), Kindle Fire Gen. 1 (Android 2.3 Gingerbread OS), Nexus 7 (Android 4.1.1).

1.4.1.3 Ports used on the network for a secure connection

The user interfaces of the WFR and its applications all use a secure (https) network connection. Please note the following ports used by the WFR and its applications::

Table 3: Application interface ports

Application	Port
WFR	1443
Web Filter	1443 appended with /login.jsp
Security Reporter (Report Manager)	8443 appended with /SR/
Security Reporter (System Configuration)	8843

To accept a security certificate for your browser type, please follow the instructions at: <http://www.trustwave.com/software/8e6/ts/wf-sec-cert.html>

1.4.2 Use the single-sign on option

By logging in to the Security Reporter using the SR Wizard username and password, the Web Filter, Security Reporter's Report Manager, and Security Reporter's System Configuration console are accessible to you via the SR's Report Manager user interface. This single sign-on option eliminates the process of choosing either the Web Filter or Security Reporter application from the WFR Welcome window and then logging in to each one.

To use the single sign-on option:

1. Log in to the Security Reporter using the SR Wizard username and password. The Report Manager user interface is available to you after logging in to the SR.
2. Go to the navigation links at the top of the Report Manager user interface and select:
 - Administration | Web Filter | (IP address) to access the Web Filter user interface
 - Administration | System Configuration to access the Security Reporter's System Configuration user interface

1.4.2.1 Default usernames and passwords for WFR applications

Default usernames and passwords for WFR applications are as follows:

Table 4: Application default credentials

Application	Username	Password
Web Filter	admin	user3
Security Reporter	admin	testpass

1.5 Database Initialization

Once the unit is installed and configured, database processing starts.



Note: On a newly installed unit, you will not be able to access the SR System Configuration user interface until Web Filter logs are transferred to the SR and its database is built. This process generally takes 24 hours.

2 Web Filter Evaluation

2.1 Configure and Test the Web Filter

2.1.1 Understand the most common and useful features

This section of the Evaluation Guide leads the evaluator, in a linear fashion, through the most common and useful features of the Web Filter, starting with the elements that should be configured first and continuing with features that require an understanding of the steps learned while configuring those first elements. Once one gets the basic flow of how filtering options are set up, it becomes quite simple to quickly make adjustments, if needed. And, the Web Filter's incredible capacity to be configured once and left alone, or to support extensive customization and specialization, make it the most versatile and network friendly filter on the market.

2.1.2 Update Libraries

Prior to reviewing the Web Filter, we recommend that you perform a complete library update; this is accomplished by going into the Web Filter Administrator console.

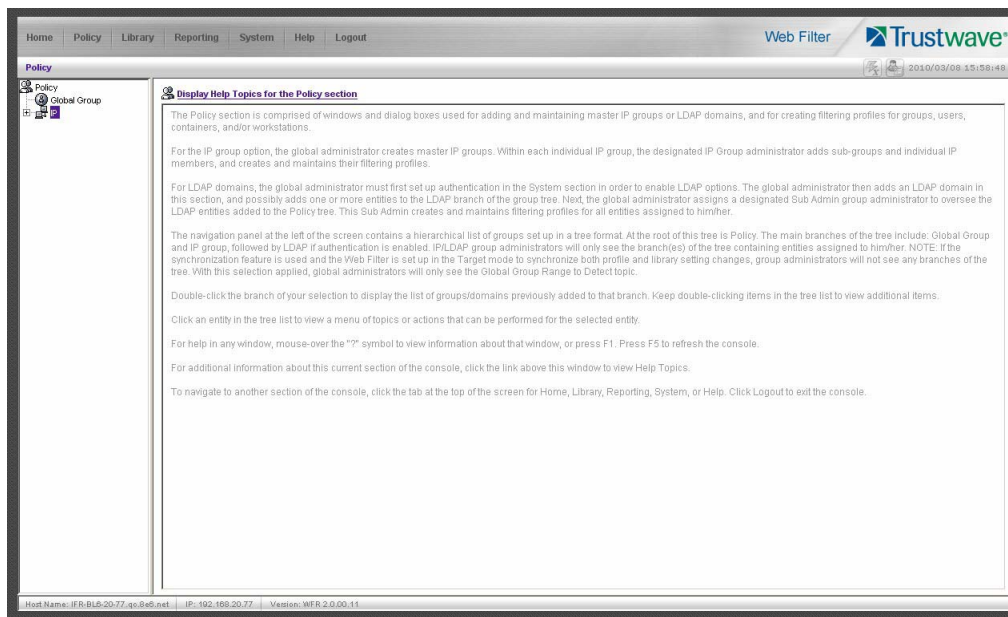
1. Click the **Library** link at the top of the screen.
2. From the navigation panel, click Updates and select Manual Update from the pop-up menu.
3. In the Manual Update to Trustwave Supplied Categories window, click the radio button corresponding to **Full URL Library Update**.
4. Click **Update Now** to begin the update process.

2.1.3 Group setup for different user types on the network

2.1.3.1 Apply different filtering levels for different types of users

Description: There are two primary Groups to understand when administering the Web Filter. The first, the **Global Group**, sets the default filtering policy for all users. In other words, the Global Group's set of filtering parameters (called a profile, to be explained later) governs every user's Internet access restrictions and permissions, *unless* a user or a group that user belongs to, has been assigned custom filtering parameters. Those exceptions to the Global Group (and there can be many) are simply called **Groups**. For example, setting aside an IP range for the sales department and altering their filtering restrictions and permissions would be considered creating a Group, likely called something as generic as Sales, and represented as an IP subset in the Global Group tree.

Figure 1: The main Policy screen



The **POLICY** administrative feature on the Web Filter allows the administrator maximum control over setting appropriate filtering levels across a broad spectrum of users. In the work environment, this could be represented by sales, accounting, research, marketing and shipping all sharing the same IP range, but requiring different levels of filtering. The POLICY feature allows the administrator to set up these groups, assign custom filtering parameters to each, and adjust those parameters as needed.

Configuration: For the purpose of evaluating the ease and effectiveness of the Web Filter's group filtering, the following example addresses the most common configuration—grouping by IP address. The Web Filter can also group by LDAP domains. Should you wish to test the group features in one of these configurations, please refer to the Trustwave Web Filter Authentication Guide, available from the Trustwave Web site. The setup is not complicated, but there are system settings required that must be initiated prior to establishing the groups in these environments, and it will be helpful and save time to work with a Solutions Engineer the first time these settings are initiated.

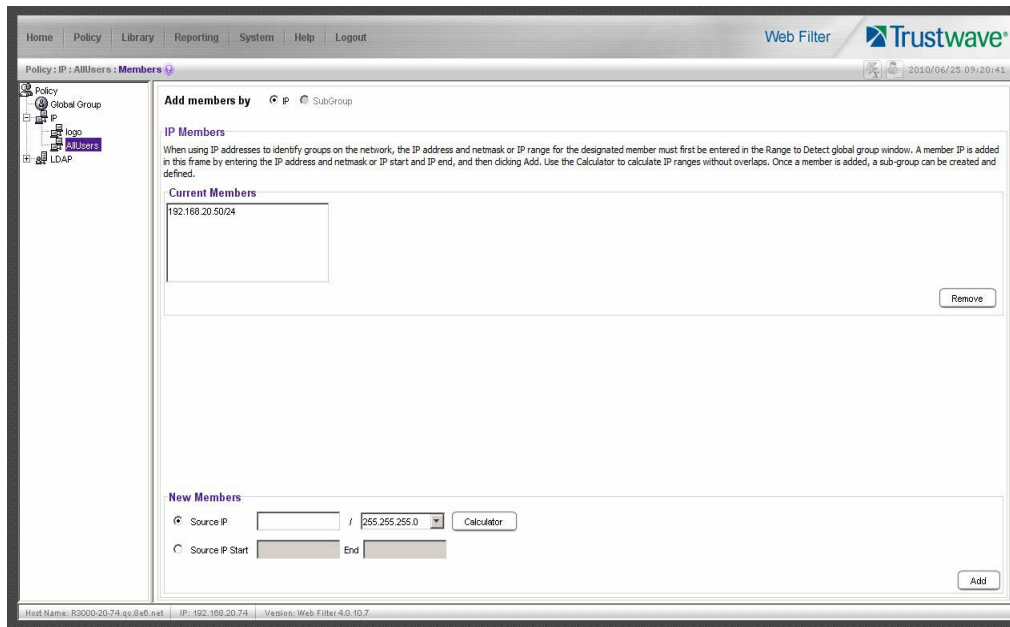
2.1.3.1.1 How to create an IP Group

1. Navigate the top level administrator console to **POLICY**.
2. Click on **IP** and select **Add Group**.
3. Provide the appropriate Group name (use AllUsers for this evaluation) and supply a password for this group. Click **OK**.

2.1.3.1.2 How to define members for this IP Group

1. Click the newly created Group and select **Members**.
2. Add members to this Group by either an IP Range or Subnet within the Range to Detect parameters of the Global Group defined earlier when setting up the Web Filter. These IP Addresses should be the IP Addresses of the computers filtered for the purposes of your testing.

Figure 2: IP Group members



2.1.3.2 Rules and Profiles: Creating and using each

Description: Rules and Profiles may seem confusing as it often appears that they are used interchangeably. And, while the administrative windows controlling the creation of Rules and Profiles are very similar, they each serve two distinct purposes.



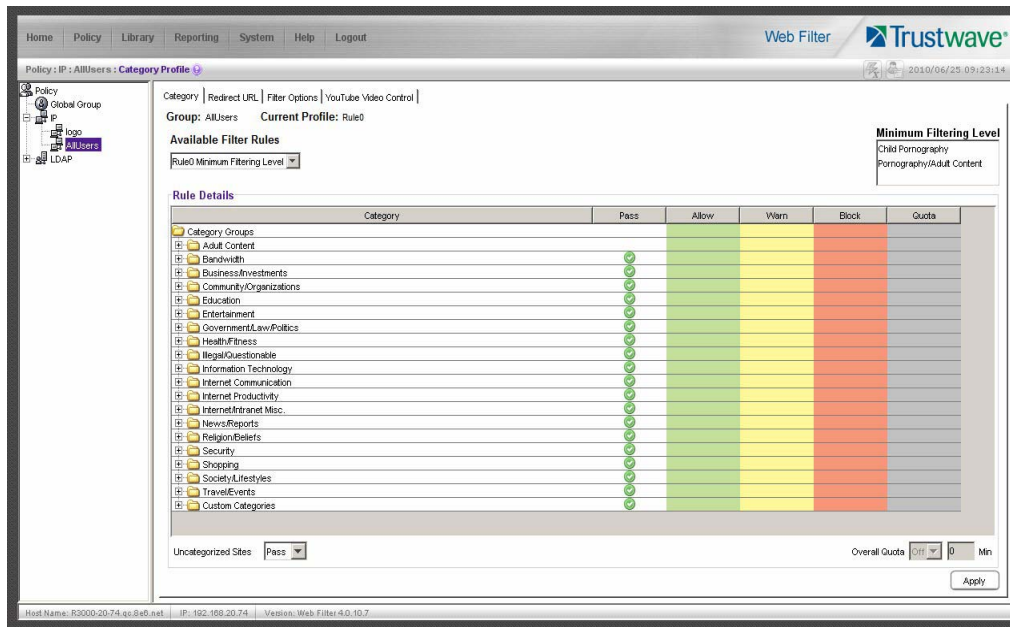
Note: The general rule of thumb is this: A Rule can be applied to a Profile, but a Profile can't be applied to a Rule. A Rule is a custom configuration of Blocked, Passed, Warned, and Always Allowed categories. A Profile contains the particular filtering parameters that are unique to a group or individual, and consists of Library Categories, Rules, Ports and numerous other filtering features that can be turned on or off.

2.1.3.2.1 How is a Rule used?

A Rule is a custom set of Library Categories. For example Rule X can be named Legal Liability and be set to block the library categories Pornography/Adult Content, Child Pornography, Explicit Art, Obscene and Tasteless, and R-Rated.

This Rule is then saved, eliminating the need to rebuild that set of Library Categories the next time that same particular set of categories needs to be applied to a group or individual. The Rule becomes part of a Profile that defines the filtering parameters for a group or individual.

Figure 3: Profile window, Rule tab



2.1.3.2.2 How is a Profile used?

A Profile defines the particular filtering parameters assigned to a group or individual. There are two kinds of Profiles. The first is the **Global Group Profile**.

The default for the Global Group Profile is set up under the Category Profile tab of the Global Group's administrative controls. Its default is set at custom and uncategorized sites are not blocked (note the Uncategorized Sites pull-down menu at the bottom of the window). The custom setting allows the administrator to immediately assign Library Categories to be passed, always allowed, warned or blocked to establish the initial default level of filtering assigned to every user (IP address) until that user (IP address) is assigned a sub-group or individual profile. ***The Global Group Profile setting doesn't use Rules, only library categories.***

The second profile is the **Group Profile**. A Group Profile is assigned to an IP Group under the Global Group and can contain filtering parameters different from the Global Group default. For example, a company may have a Global Group Profile that blocks access to all sites in the earlier Legal Liability Rule example, i.e. Pornography/Adult Content, Child Pornography, Explicit Art, Obscene and Tasteless, and R-Rated. That means every employee (or every computer the employees use) is subject to those filter parameters. However...

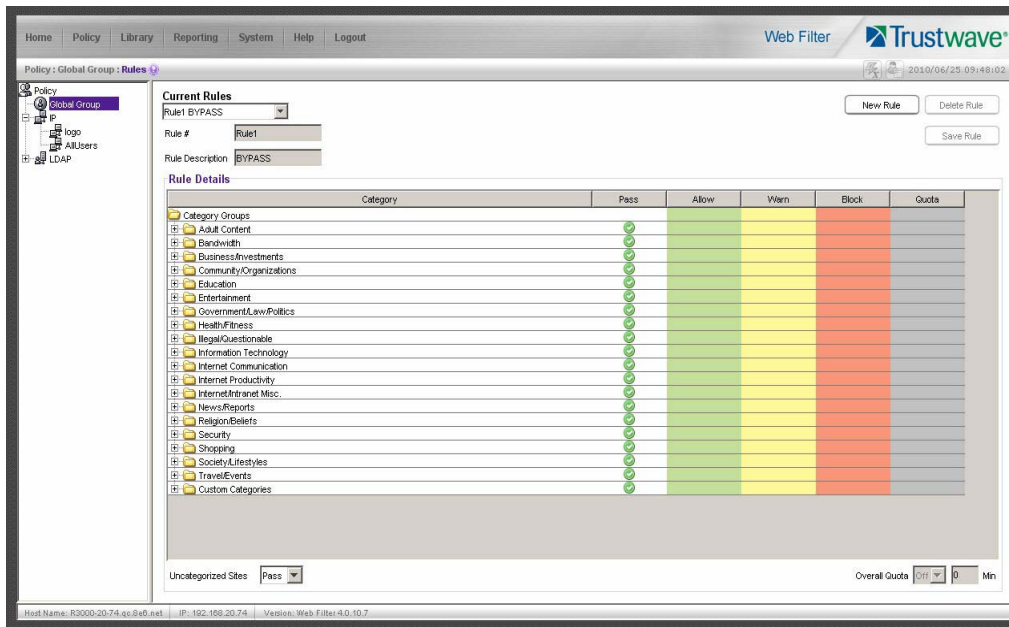
Let's say the employees in the marketing department need to access photo services, online publications and other sites that might contain some adult content—or at least suggestive images. An administrator can set up a Group that is subject to a custom profile, which might be called Marketing, which is different from the Global Group Profile, to allow access to the R-Rated library category. This group, or range of IP

addresses, now exists within the Global Group, but with different filtering criteria. The rest of the Global Group (all other IP addresses) remain filtered by the default Global Group Profile, which includes R-Rated.



Note: Different doesn't necessarily mean that a group is no longer filtered by the library Categories in the Global Group Profile. In fact, different may mean the group is filtered by several categories in addition to those in the Global Group Profile. There are many ways a Group can be set up. The thing to remember is that a Group is set up to provide a different profile from the Global Group.

Figure 4: Rules window



The Rules window displays when Rules is selected from the Global Group menu. This window is used for adding a filtering rule when creating a filtering profile for an entity. By default, Rule1 BYPASS displays in the Current Rules pull-down menu. The other choices in this pull-down menu are Rule2 BLOCK Porn, Rule3 Block IM and Porn, Rule4 Trustwave CIPA Compliance (which pertains to the Children's Internet Protection Act) and Rule5 Block All. By default, Rule1 displays in the Rule # field, BYPASS displays in the Rule Description field, and Uncategorized Sites are allowed to pass.



Note: Uncategorized sites are those sites which have not been identified and placed within one of the 100+ categories in the Web Filter's Library database. The Pass default will allow those URLs to be viewed. Block will prevent those sites from being viewed.

2.1.3.2.3 How to create a new Rule

1. From the top level administrator console, select **POLICY**.
2. Click Global Group and select Rules.
3. In the Rule Details frame click **New Rule** to populate the **Rule #** field with the next consecutive rule number available.
4. Enter a unique **Rule Description** that describes the theme for that Rule.
5. By default, all library categories are included in the Pass Categories column. All categories are grouped in logical Category Groups. For example, in the Adult Content category group you would find the cate-

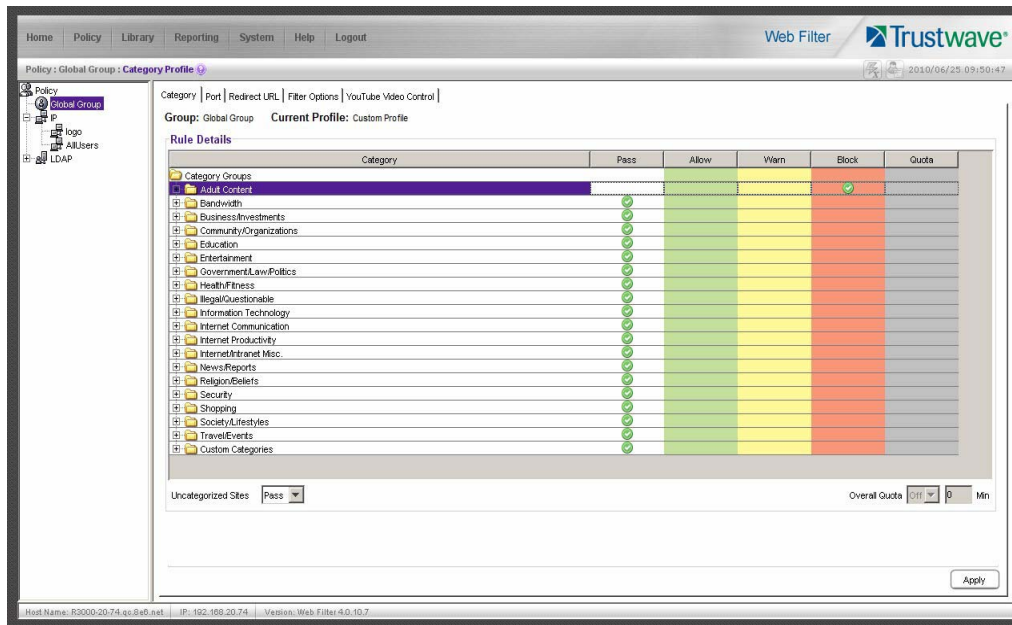
gories Child Pornography, Explicit Art, Obscene and Tasteless, R-Rated, and Pornography. To move all categories within a category group to another column, select the column next to the category group. To move a single category, expand the category group, and select the column for just that category.

- Double click the Block column to move the library category to the blocked categories column.
 - Double click the Allow column to move the library category to the always allowed column.
6. Select Pass, Warn, or Block to specify whether all **Uncategorized Sites** should pass, warn the user, or be blocked.
 7. Click **Save Rule** to include your Rule to the list that displays in the pull-down menu.

2.1.3.3 Global Group Profile

The Global Group Profile window displays when Global Group Profile is selected from the Global Group menu.

Figure 5: Global group profile, Category tab



2.1.3.3.1 Set the Global Group Profile

The Category Profile displays by default when Global Group Profile is selected from the Global Group menu. This window is used for selecting library categories that will be passed, warned, always allowed or blocked for the Global Group Profile.

By default, Custom Profile displays in the Available Filter Levels pull-down menu, and **Uncategorized Sites** are allowed to pass.

2.1.3.3.2 Create, edit a list of selected Categories

To define which categories will be passed, warned, always allowed or blocked in the Global Group Profile:

1. Select a library category from the Pass categories column.

2. Click in the appropriate column:

- Double click the Block column to move the library category to the blocked categories column.
- To remove a library category from the Block column, double click the Pass column.
- Double click the Allow column to move the library category to the always allowed column.

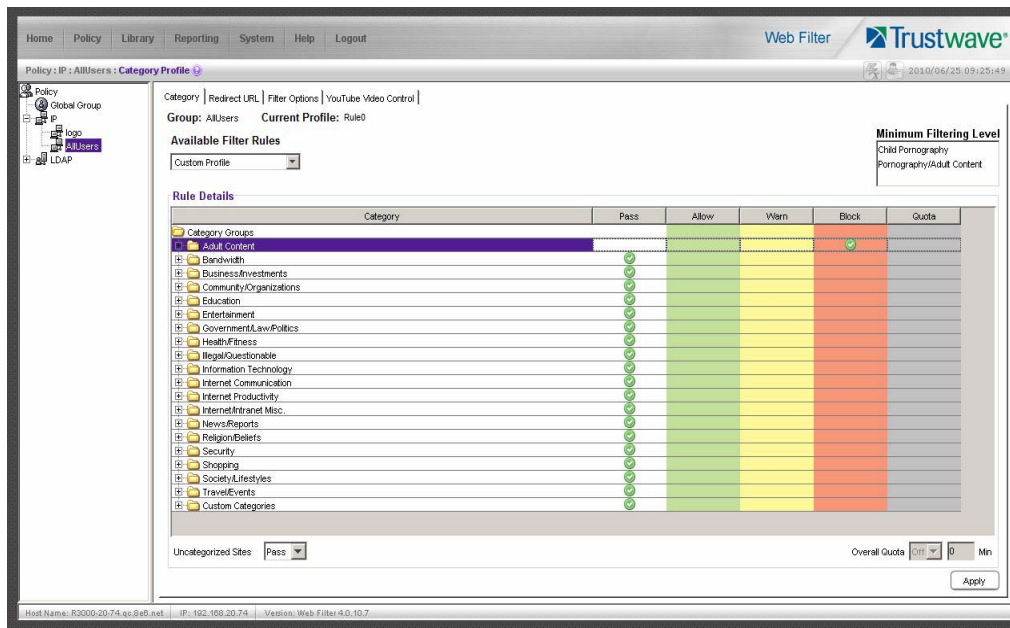
3. Choose Pass, Warn or Block to specify whether **Uncategorized Sites** should pass, warn the user, or be blocked.

4. Click **Apply** to save the settings.

2.1.3.4 Group Profile

The Group Profile window displays when Group Profile is selected from an IP Group.

Figure 6: Group Profile window, Category Profile tab



2.1.3.4.1 Set the Group Profile

Setting up a Group Profile is exactly the same as setting up the Global Group Profile, except that Rules can be used to define the Profile.

Category Profile displays by default when Group Profile is selected from an IP Group. This tab is used for selecting library categories that will be passed, warned, always allowed or blocked for the Group filtering profile.

By default, Rule0 Minimum Filtering Level displays in the Available Filter Levels pull-down menu, and Uncategorized Sites are allowed to pass.

To set the Profile of the Group, the administrator can either select a pre-set Rule or go through the process of moving library categories into the Pass, Allow, Warn or Block fields—or use both Rules and library Category selections to create a unique profile.

Selecting the library categories to be in the Pass, Allow, Warn or Block columns is just like configuring the Global Group Profile library Categories.

2.1.3.4.2 Create, edit a list of selected Categories for a Group Profile

To define which categories will be passed, warned, always allowed or blocked in the Global Group Profile:

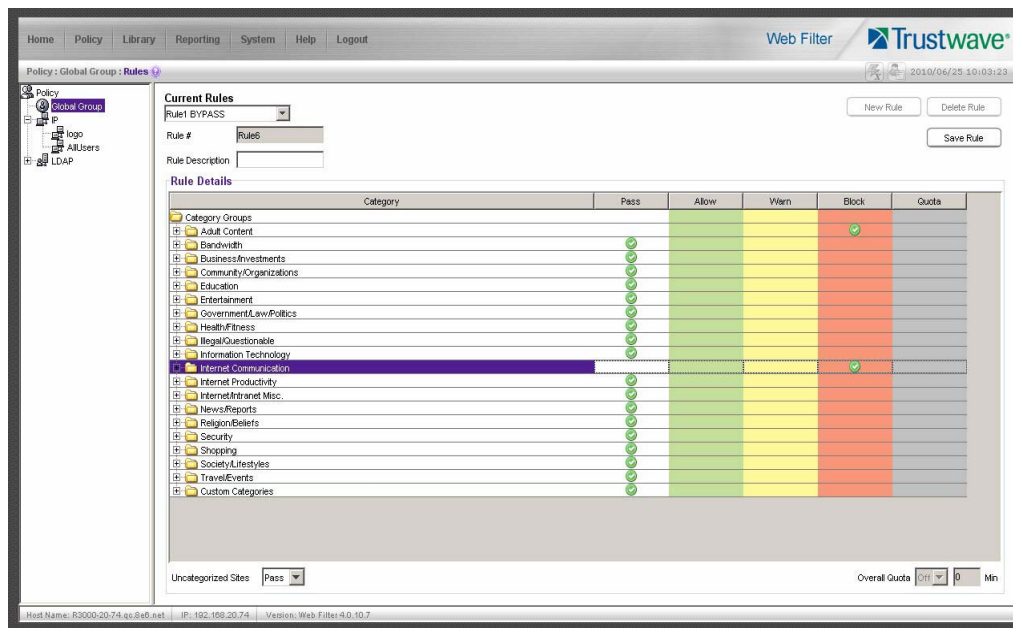
1. Select a library category from the Pass categories column.
2. Click in the appropriate column:
 - Double click the Block column to move the library category to the blocked categories column.
 - To remove a library category from the blocked categories column, double click the Pass categories column.
 - Double click the Allow column to move the library category to the always allowed column.
 - To remove a library category from the always allowed column, double click the Pass column to move that category back to the pass categories column.
3. Choose Pass, Warn or Block to specify whether **Uncategorized Sites** should pass, warn the user, or be blocked.
4. Click **Apply** to save the settings.

2.1.4 Group settings tests

2.1.4.1 Test the Rules and Profiles feature

To test the Rules and Profiles feature, first define a Rule.

Figure 7: Rules window



1. Select **Rules** under Global Groups.

2. Click **New Rule** (the Rule # will reflect the next sequential number available for a rule).
3. Move categories from Pass categories to Allow, or Block as desired. Leave categories that don't need to be blocked in Pass.



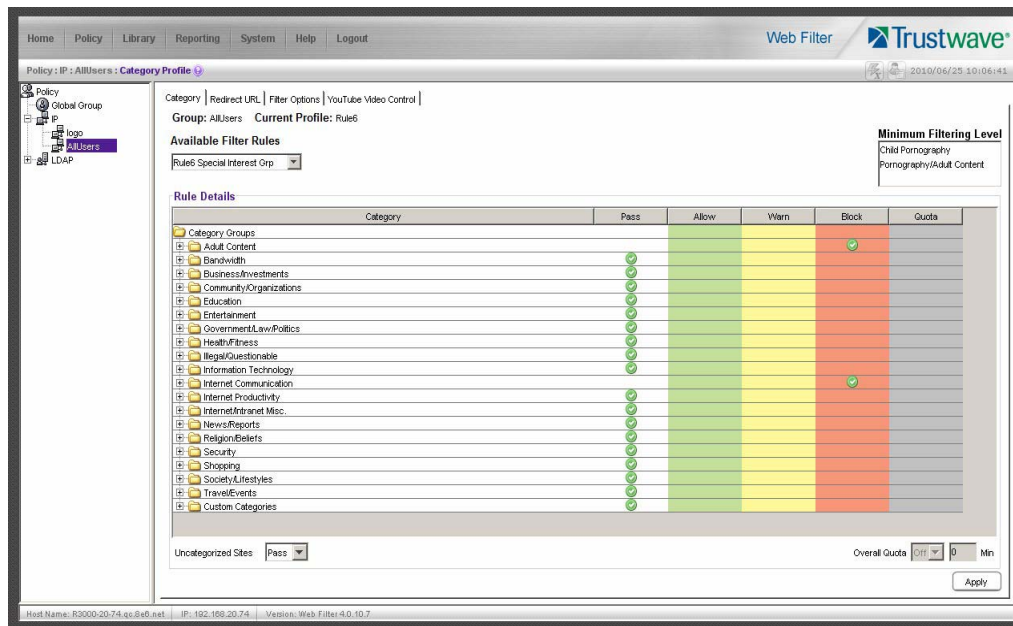
Note: For the purposes of the evaluation, it is recommended that you only place two categories in Block and Allow. Leave the remainder in Pass.

4. Specify whether **Uncategorized Sites** should pass or be blocked.
5. Give the Rule a Description/Name.
6. Click **Save Rule**.
7. Select Yes when asked if you want to add the Rule.

2.1.4.2 Test the Rule

To test the Rule, apply it to an IP Group.

Figure 8: IP group profile window with rule applied



1. Select AllUsers from the IP Groups.
2. Select Group Profile.
3. In the **Available Filter Levels** field, select the Rule you created.
4. Click **Apply** in the bottom right corner.
5. Access the Internet from an IP address within the Sales group.
6. Attempt to access a Web site obviously included within the blocked categories contained in the Rule. The site will be blocked.

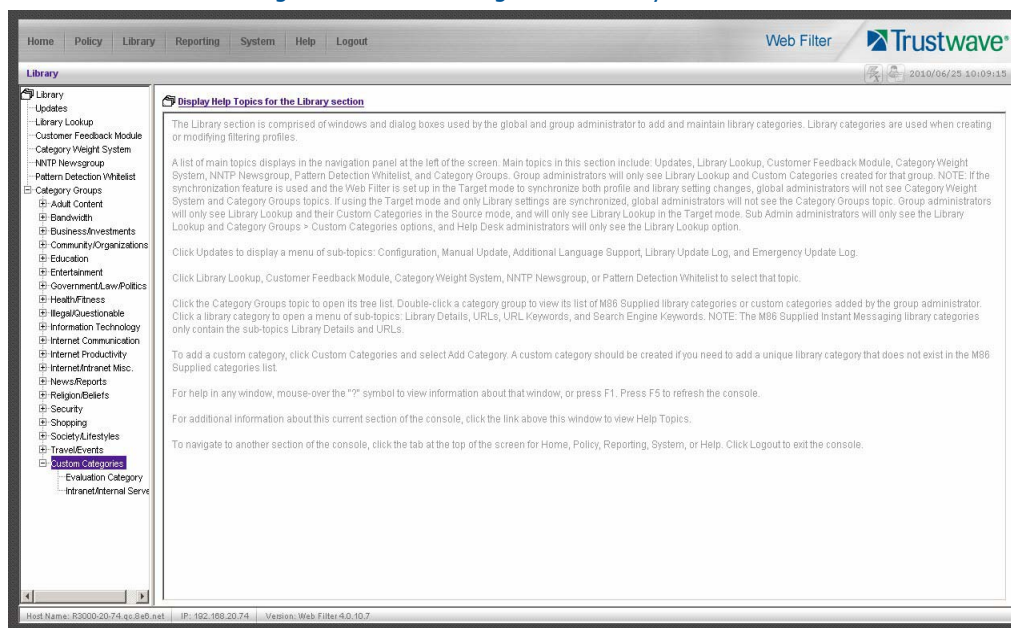
7. Access the Internet via an IP address *not* included in the Sales range and attempt to access the same URLs. Access *will not* be blocked.
8. Repeat with several Web sites and different categories, if desired.

2.1.5 Custom Categories

2.1.5.1 Create and configure a Custom Category

Description: The Web Filter allows an administrator to create a new category not listed among the 100+ options in the Library Categories. With literally tens of millions of URLs researched and screened among those existing categories, it might seem like a case of overkill to create a new one, but many of the most useful and powerful features of the Web Filter depend on the creation of Custom Categories.

Figure 9: Custom Categories in Library tree menu



2.1.5.1.1 How to create a Custom Category

1. Navigate the top level administrator console to **LIBRARY**.
2. Click **Custom Categories** and select Add Category.
3. Provide a name and description for your custom category.
4. For evaluation purposes, call the new category Evaluation Category.
5. Add a Short Name description (7 characters maximum) and click **Apply**.

2.1.5.1.2 How to add URLs to the Custom Category

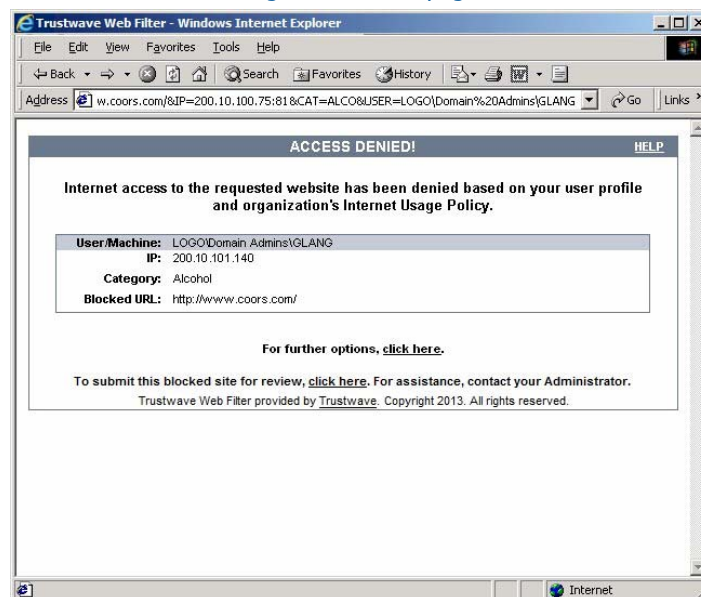
1. Select the newly created Custom Category.
2. Select the **URLs** option. The Web Filter provides the interface to add and remove sites from the custom category.

3. Type in a URL you want to add.
4. Click **Add**. Wait for a moment while the Web Filter searches through all URLs in its Library database (including IP addresses) to find URL and IP matches. Matches are listed in the window.
5. Select all URLs and IP addresses you want to add from the list (use Ctrl and Shift keys to allow multiple selects).
6. Click **Apply Action**.
7. Repeat for each URL.

2.1.5.1.3 Custom Category setup and usage test

1. Create a custom category called Evaluation Category.
2. Add any three URLs per the previous configuration instructions.
3. Select **POLICY** from the top level administrator navigation.
4. Click Global Group and select Global Group Profile.
5. In the Category Profile tab, from the Pass column, select the Evaluation Category custom category you created and move it to the Block column.
6. Move any other category in the Block column to the Pass column.
7. Select Pass from Uncategorized Sites.
8. From an IP address contained within the Global Group range, attempt to access any of the URLs included in the Evaluation Category. Access is blocked.
9. Attempt to access a URL not in the Evaluation Category. Access is allowed.

Figure 10: Block page

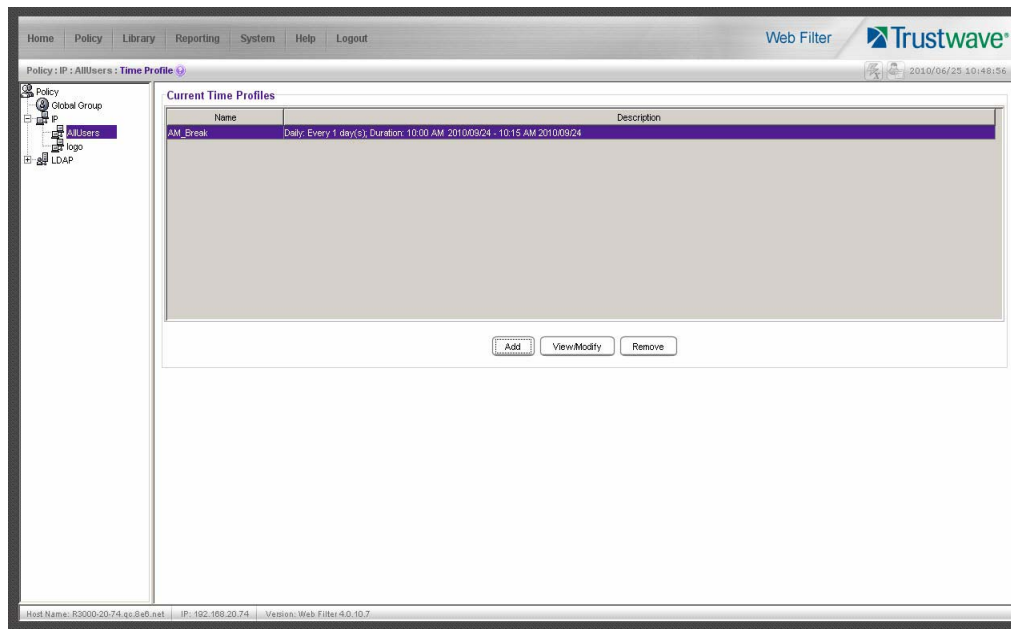


2.1.6 Filtering profile features

2.1.6.1 Time Profile feature

Description: The Time Profile feature lets the administrator set up a profile for any user or group to run at a scheduled time period. A user or group can have multiple time profiles, and these can be set to run at various intervals of time throughout a day, week, month, or year.

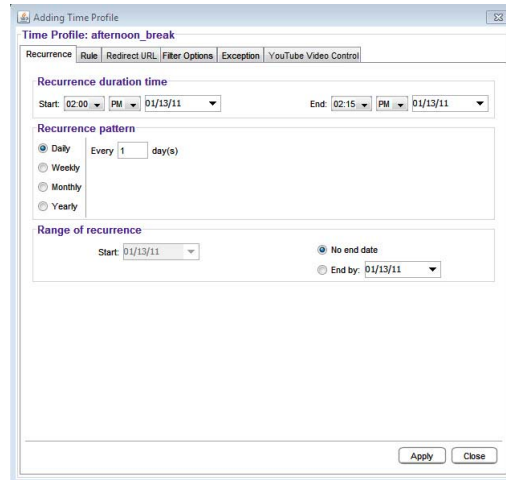
Figure 11: Time Profile window



2.1.6.1.1 Set up a Time Profile

1. Select **POLICY** from the top level administrator console.
2. Choose AllUsers from the IP Groups, and select Time Profile from the menu.
3. Click **Add**, enter a name for the Time Profile, and then click **OK**.
4. Notice that the **Start** time is pre-populated with the closest 15-minute time period and the **End** time period is pre-populated with the time period an hour after the Start time. For the purpose of this exercise, change the End time to be 15 minutes after the Start time.

Figure 12: Adding Time Profile window



5. Click the Rule tab.
6. Double click the **Society/Lifestyles** Category to open it.
7. Find Alcohol, double click in the **Block** column, and click **OK**.



Note: In order to perform the test that follows, be sure the Alcohol category isn't blocked in any other profile for this group.

8. Click **Apply** in the bottom right corner, click **Yes**, and then click **OK**.
9. Click **Close**.

2.1.6.1.2 Test the Time Profile

1. From an IP address within the Sales group, access countless alcohol-related Web sites on the Internet for a 15-minute period—coors.com, absolut.com, budweiser.com, wine.com, etc. You should receive a block page when attempting to access these pages.
2. After the 15-minute period has ended, attempt to access URLs in the Alcohol category; you should be able to access these pages.

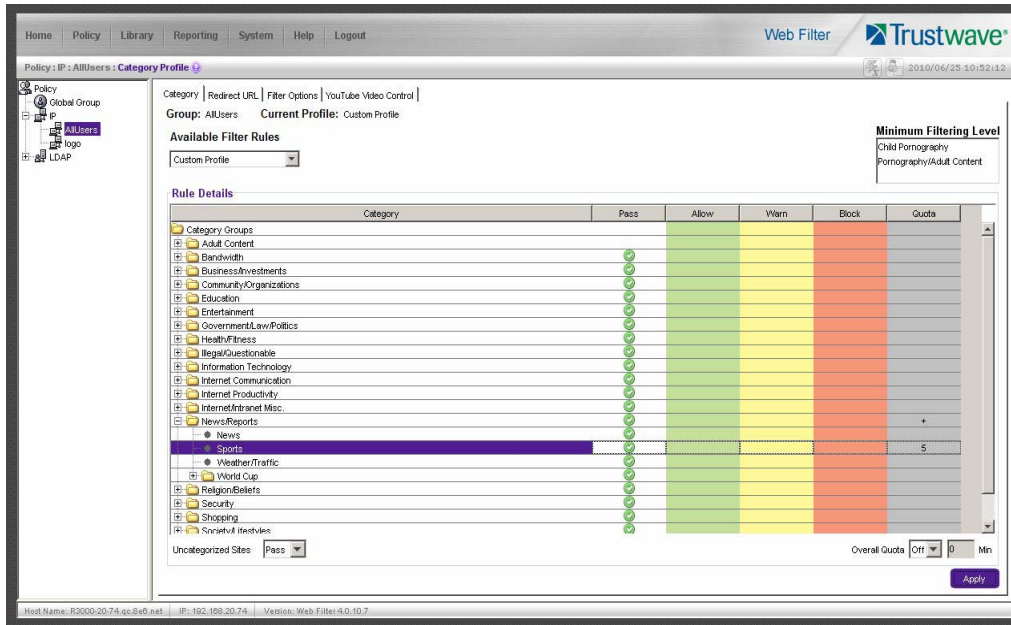
2.1.6.2 Quota feature

Description: The Quota feature restricts the amount of time a user can spend in a passed category. When the user reaches 75 percent of time in a quota-designated category, the quota notice page pops up to warn the user about this information. If 100 percent of quota time is attained, the user receives a quota block page and cannot access that category until quotas are reset.



Note: If the Overall Quota is specified in the profile, the user's total quota time for all quota-marked categories is capped by the number of minutes entered in the Minutes field.

Figure 13: Quota time shown in Quota column and Overall Quota enabled



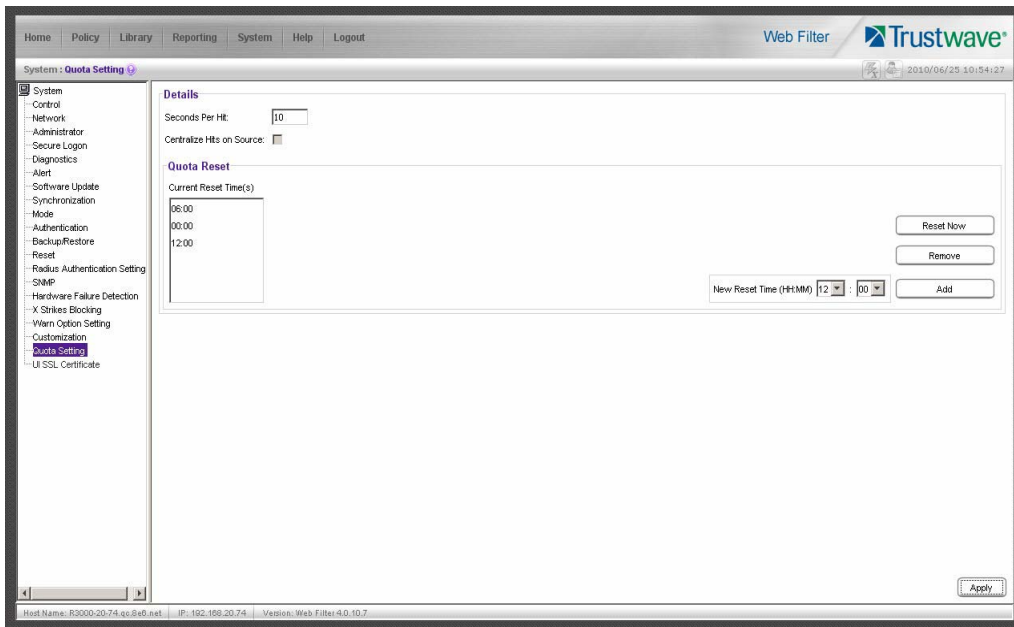
2.1.6.2.1 Set up the Quota feature

1. Select **POLICY** from the top level administrator console.
2. Choose AllUsers from the IP Groups.
3. Double click the **News/Reports** Category to open it.
4. Find Sports, double click in the Quota column, and enter 5.
5. Click **Apply** in the bottom right corner.

2.1.6.2.2 Test the Quota feature

1. From an IP address within the Sales group, access countless sports-related Web sites on the Internet for a five-minute period—espn.com, sportsillustrated.cnn.com, tennis.com, soccer.com, etc. During the course of the five minute period, you should receive a Quota Notice page informing you that 75 percent of quota time has been attained.
2. Continue accessing sports-related Web sites. After the five-minute period has elapsed, you should receive the Quota Block page informing you that your access to the Sports Category is now blocked.

Figure 14: Quota Setting window

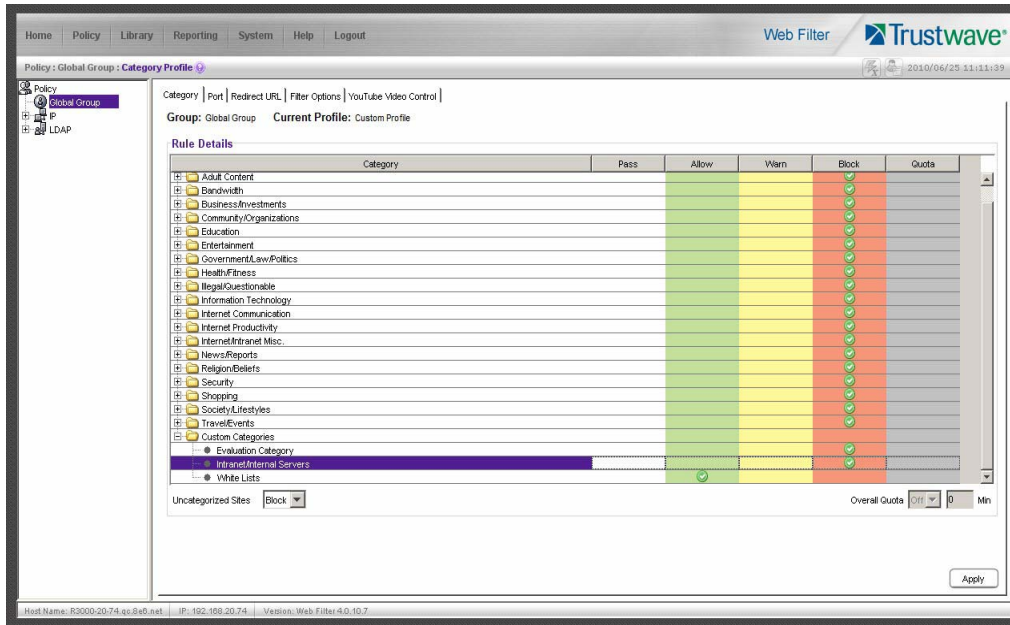


3. To reset the quota for your profile, first select **SYSTEM** from the top level administrator console.
4. Next choose Quota Setting.
5. Click **Reset Now** and then click **Apply**.
6. Using the same IP in the Sales group, attempt to access sports-related sites; you should be able to access these URLs again.

2.1.6.3 White List feature

Description: White lists are effective when a particular group requires tight control over content options. For example, rather than spend hours determining what employees in shipping shouldn't be viewing, it is much easier to define only the things they *can* view. Restricting that group to specific URLs provides a way to ensure the only Web sites visited are those required for work—without requiring administrators to keep up with employees who find creative ways to bypass black lists.

Figure 15: White list rule setup



2.1.6.3.1 How to create and configure a White List

1. Create a custom category called White Lists.
2. Add a couple of URLs that students might access for reference.
3. Select **POLICY** from the top level administrator navigation.
4. Click Global Group and select Global Group Profile.
5. In the Category Profile tab, select the White Lists custom category you created from the Pass categories column. Double click the Allow column.
6. Block all other categories by double clicking the Block column.
7. Select Block from Uncategorized Sites pull-down menu.
8. Click **Apply**.

2.1.6.3.2 Test the White List

After completing steps 1-8 above, then:

1. From an IP address contained within the Global Group range, attempt to access any of the URLs included in the Evaluation Category. Access is allowed.
2. Attempt to access a URL not in the White Lists category. Access is denied.

2.1.6.4 Warn feature

The Warn feature allows the administrator to warn a user that sites within a specific category may violate the acceptable use policy, without actually blocking them from the site outright. The user will be prompted with a warning about the possibility of AUP violation. If the visit to the site is for appropriate business use,

the user can elect to continue on to the site. If the user feels that they should not continue on to the site, they can also elect to do this.

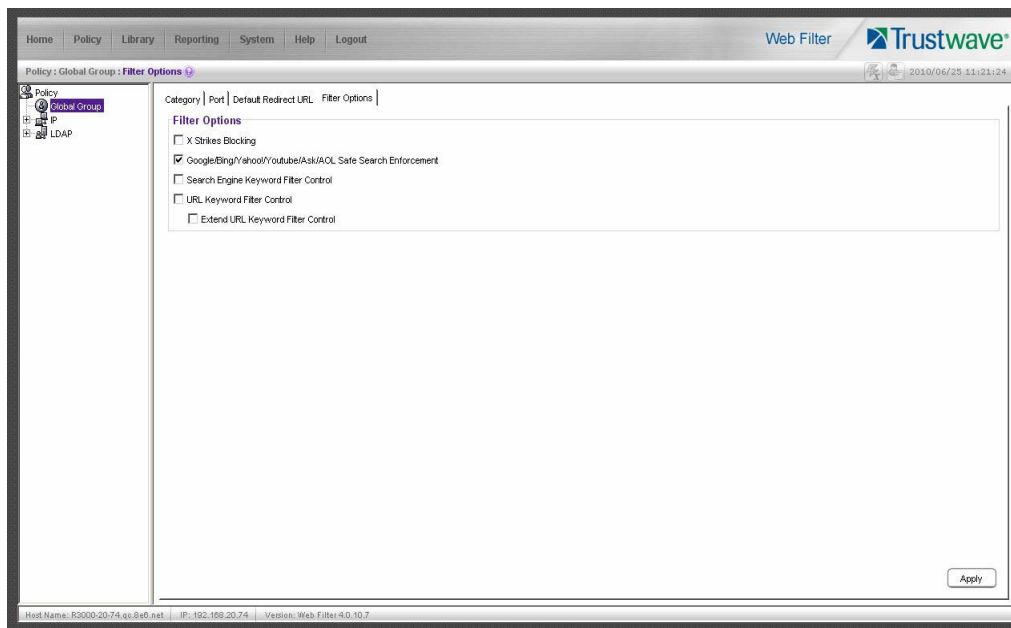
2.1.6.4.1 How to test the Warn feature

1. Select the category you wish to Warn.
2. Double click the Warn column next to that category.
3. Visit that category on a filtered PC.

2.1.6.5 Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement

Description: Google, Bing, Yahoo!, YouTube, Ask, and AOL have very effective safe search features that can be activated to ensure search results do not contain sexually explicit material. Unfortunately, safe search can be deactivated in the preference settings of each search engine. The Web Filter allows these filters to stay activated—with the settings remaining unchangeable except by the administrator of the Web Filter.

Figure 16: Safe Search Enforcement Filter Options



2.1.6.5.1 How to configure the Safe Search Enforcement feature

1. Select **POLICY** from the top level administrator console.
2. Click Global Group and select Global Group Profile.
3. Select the Filter Options tab.
4. Select the **Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement** check box.
5. Click **Apply**.

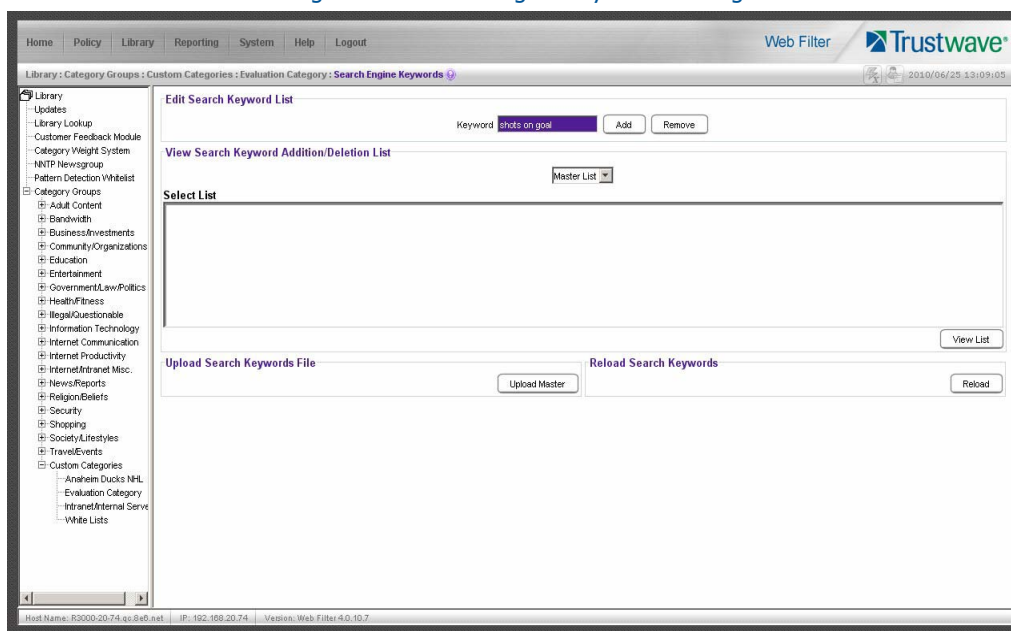
2.1.6.5.2 How to test the Safe Search Enforcement feature

1. Configure the Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement feature.
2. Access Yahoo! from an IP address within the Global Group range.
3. Manually set the Yahoo! search settings to the lowest filtering option.
4. Search using the term *playboy*. Content is filtered by Yahoo!
5. Repeat for Google, Bing, YouTube, Ask, and AOL.

2.1.6.6 Search Engine Keyword Filtering

Description: There are a number of words and phrases that clearly won't be used to find business-related content on the Web. With Search Engine Keyword Filtering administrators can stop a search before it even starts (to cause trouble). The Web Filter allows administrators to add words or phrases, up to 75 characters in length (alphanumeric), to shut down access to restricted content right at the point an employee clicks search. These words and phrases can be added either one at a time or by uploading a text file. Instead of questionable content and/or images, a block page appears.

Figure 17: Search Engine Keyword filtering



2.1.6.6.1 How to configure Search Engine Keyword Filtering

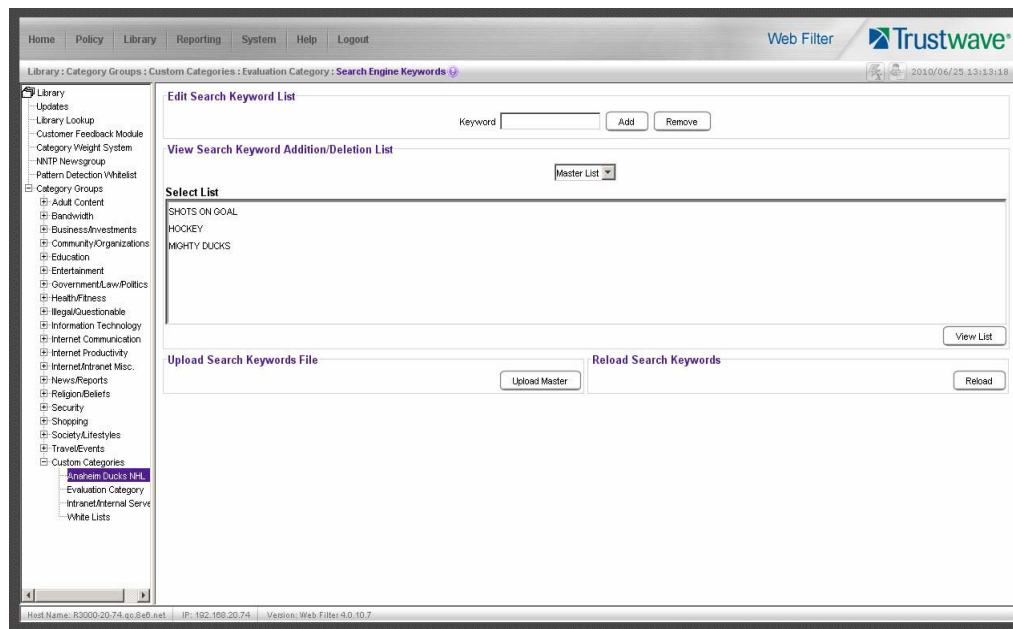


Note: Search Engine Keyword Filtering must be activated as part of a custom category.

1. Select **LIBRARY** from the top level administrator console.
2. Create a Custom Category (or add Search Engine Keyword Filtering to an existing custom category).
3. Select the Custom Category and choose Search Engine Keywords.

4. Type in a keyword and click **Add**.
5. Repeat and follow screen prompts.
6. Select **POLICY** from the top level administrator console.
7. Click on Global Group and select Global Group Profile.
8. Click the Filter Options tab.
9. Activate the **Search Engine Keyword Filter Control** check box.
10. Click **Apply**.

Figure 18: Adding Search Engine Keywords



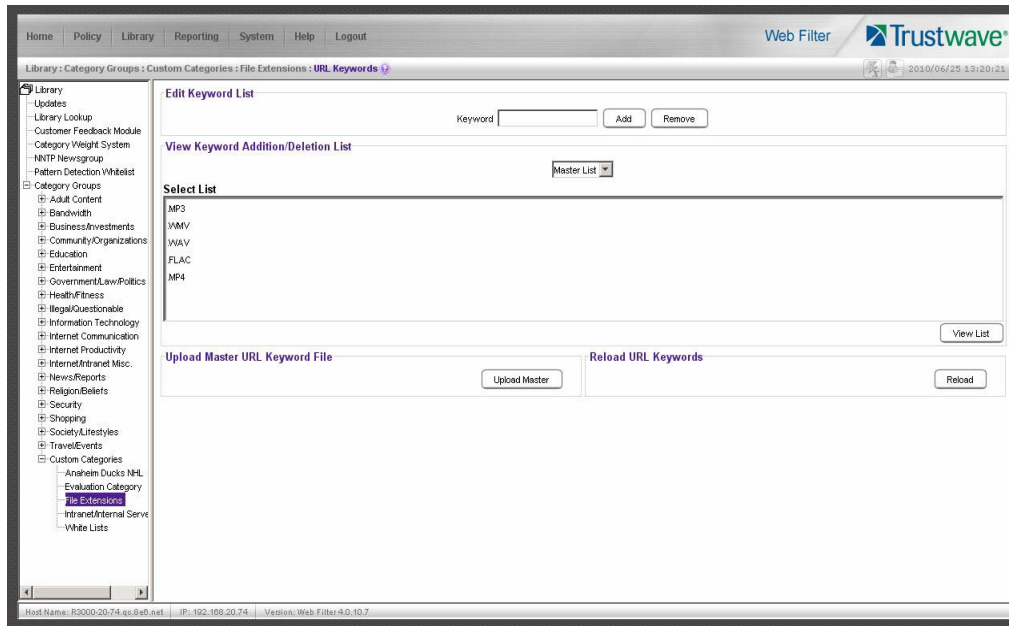
2.1.6.6.2 How to test Search Engine Keyword Filtering

1. Create a custom category called Keyword Filtering, using the keywords playboy, sex and porn.
2. Activate **Search Engine Keyword Filtering** in the Global Group Profile.
3. In the Global Group Profile, select the Category tab.
4. Move the Keyword Filtering category setup selection from Pass to Block.
5. Click **Apply**.
6. Access Yahoo! from an IP address within the Global Group range.
7. Enter playboy into the search field and click search. The search will be blocked.
8. Repeat for sex and porn.
9. Test in Google, Bing, YouTube, Ask, and AOL as well.

2.1.6.7 Attachment filtering

Description: Unchecked and unmanaged, the download of attachments can bring a network to its knees. The Web Filter's Attachment Filtering feature identifies the download of a file as soon as it's initiated, and blocks the download.

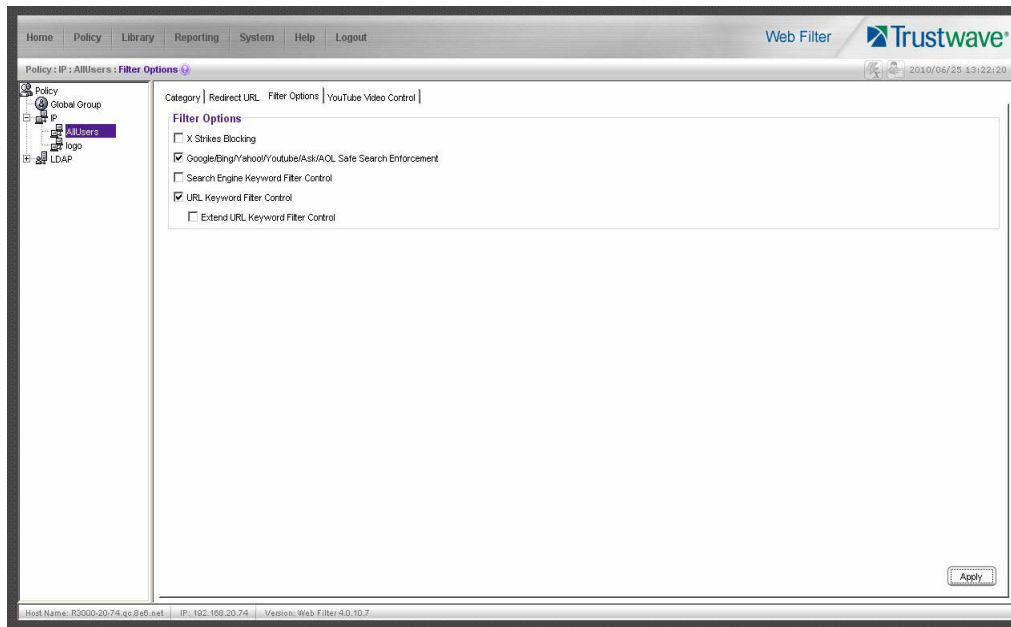
Figure 19: Attachment filtering setup in URL Keywords



2.1.6.7.1 How to configure attachment filtering

1. Select **LIBRARY** from the top level administrator navigation.
2. Add a custom category and call it **File Extensions**.
3. Select URL Keywords from the newly-created File Extensions custom category.
4. Add a file extension in the Keyword field and click Add. (When adding the file extensions, make sure you add them with the period before the keyword, e.g. type .mp3 in the keyword field, not mp3).
Keep adding until you have entered all the desired file extensions.
5. Click **Reload** to reload the library.
6. Select **POLICY** from the top level administrator navigation.
7. Click Global Group and select Global Group Profile.
8. Select the Filter Options tab.
9. Enable **URL Keyword Filter Control** and click **Apply** to save.
10. Select the Category tab. Add the File Extensions custom category (found in the Pass column) to the Block column.

Figure 20: Attachment filtering setup in Filter Options tab



2.1.6.7.2 How to test attachment filtering

1. Configure the File Extensions custom category.
2. Enable URL Keyword Filter Control in the Global Group Profile.
3. Access the Internet from an IP address within the Global Group range.
4. Go to a Web site with file downloads (mp3, shareware, movies, etc.).
5. Attempt to download a file. The attempt will be blocked.

2.1.6.8 Wildcard filtering

Description: Online communities such as myspace.com continually add numerous sub-domains to house the profiles of their fast growing communities. Rather than manually adding each and every individual domain to the library on an ongoing basis, the Web Filter can accept a wildcard to block these types of sites more efficiently. For example, adding `http://*.myspace.com` (where the asterisk [*] is the wildcard indicator) to a customized category's URL list will ensure that anything on myspace.com will be blocked.

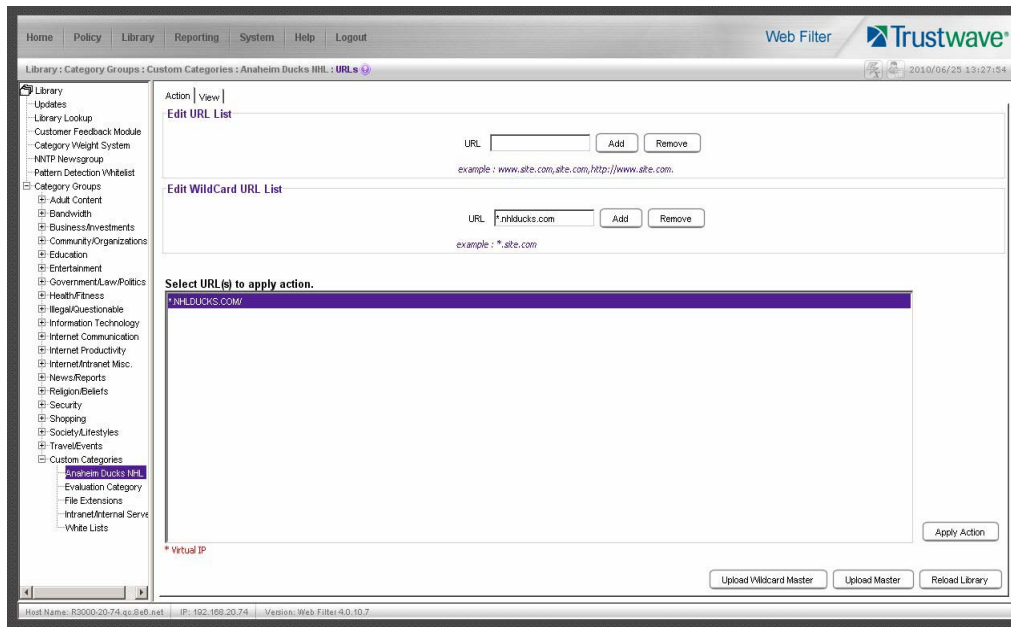


Caution: If a specific URL was added to a custom library category that is **not** set up to be blocked, and a separate wildcard entry containing a portion of that URL is added to a category that **is** set up to be blocked, the end user will be able to access the non-blocked URL but not any URLs containing text following the wildcard.

For example, if `http://www.cnn.com` is added to a category that is **not** set up to be blocked, and `*.cnn.com` is added to a category that **is** set up to be blocked, the end user **will** be able to access:

`http://www.cnn.com` since it is a direct match, but **will not** be able to access `http://www.sports.cnn.com`, since direct URL entries take precedence over wildcard entries.

Figure 21: Wildcard filtering



2.1.6.8.1 How to configure wildcard filtering

1. Go to **LIBRARY** in the top level administrator navigation.
2. Click an existing custom category or create a new one.
3. Select URLs from that category to add the wildcard URL.
4. In the URL text field enter the site in the format of *.site.com and click **Add**.
5. Highlight the newly added wildcard URL and click **Apply Action**.
6. Continue with any other wildcards you want to add.
7. Click **Reload Library** for changes to take effect.



Tip: Wildcards are to be used for blocking only. They are not designed to be used for the exceptions function or the always allowed white listing function. The minimum number of levels that can be entered is three (*.yahoo.com) and the maximum number of levels is six (*.mail.attachments.message.yahoo.com).

2.1.6.8.2 How to test wildcard filtering

1. Create a custom category called Wildcards.
2. Add the following URLs (or any three URLs) per the previous configuration instructions:
 - a. *.playboy.com
 - b. *.myspace.com
 - c. *.8e6.com
3. Select **POLICY** from the top level administration navigation.

4. Click Global Group and select Global Group Profile.
5. In the Category tab, move the Wildcards custom category you created from the Pass column to the Block column.
6. Select the Block option from **Uncategorized Sites**.
7. From an IP address contained within the Global Group range, go to Google.
8. Initiate a search for any of the domains (using keywords playboy, myspace, and 8e6. You should get numerous sub-domain choices to select.
9. Attempt to access a link from Google. Access is denied.

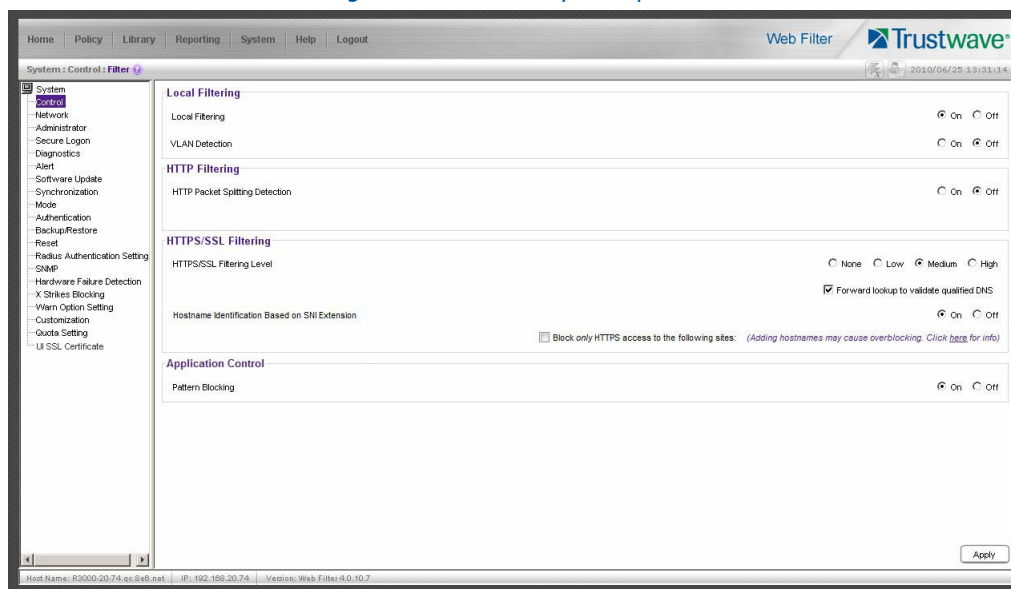
2.1.7 Configure, test, block services

2.1.7.1 Anonymous proxies

Description: Web-based anonymous proxy services provide a method to bypass Web filters. Administrators can block the **Web-Based Proxies/Anonymizer** library Category to keep employees away from sites that offer free anonymous proxy services. As a second layer of protection, the Web Filter also offers **Proxy Pattern Blocking**.

Proxy Pattern Blocking prevents users from bypassing the filter if they try to use (unencrypted) Web and client-based proxies. Therefore, if the site is not categorized as Web-Based/Anonymous Proxies, the Web Filter will still be able to block access to the site based on signature files in the Trustwave Database.

Figure 22: Block anonymous proxies



2.1.7.1.1 How to configure anonymous proxies

1. Select **SYSTEM** from the top level administrator console.
2. Click **Control** and select Filter.

3. Set the **Pattern Blocking** radio button to **On**.
4. Select **POLICY** from the top level administrator console.
5. Click Global Group and select Global Group Profile.
6. Move the **Web Based/Anonymous Proxy** category from the Pass column to the Block column.
7. Click **Apply**.

2.1.7.1.2 How to test anonymous proxies

1. From an IP address in the Global Group range, go to <http://proxy.org> and click on Free Proxy Form.
2. Enter any URL and select GO. The request is routed through anonymous proxies and is blocked.

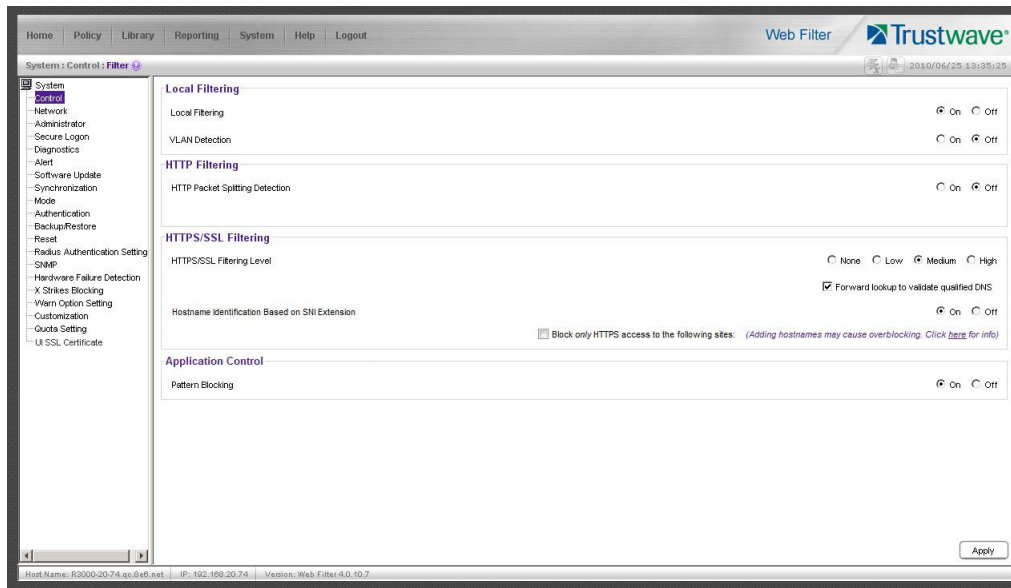
The Web Filter blocks these proxy types using the Proxy Pattern Detection feature:

- PHPproxy form (unencrypted): v0.3 and 0.4
- CGIProxy - HTTP/FTP proxy in a perl based CGI script (unencrypted) including CGI-redirects: v2.0.1 and 2.1beta6
- Perl based proxy module: v5.8 (backward compatible)
- Accelerator and Split Proxies: GWA v0.2.64 and higher
- Anonymous and Transparent Proxies (unencrypted) used in combination with PHP, CGI, Perl, Accelerator
- Hopster (HTTP Tunnel): v17
- GCD related proxies: UltraReach (web-based), UltraSurf v6.9 and FreeGate v6.0

2.1.7.2 Block IM, P2P applications and streaming media

Description: The Web Filter provides Peer-to-Peer (P2P) and Instant Message (IM) blocking. Peer-to-Peer and Instant Messaging pose significant challenges to administrators due to the risks of content type that can be passed on via these tools (images and video), as well as the ease by which these enable malicious code and viruses to circumvent many networks. Additionally, sites that offer IPTV programming, streaming video, streaming radio Internet programming and other such streaming media create a tremendous demand for network resources and can severely impact network performance. In addition to blocking IM and P2P applications, the Web Filter also logs user attempts to run these applications through the Web Filter's Intelligent Footprint Technology (IFT). IFT blocks these applications based on the traffic patterns they generate.

Figure 23: Block patterns



2.1.7.2.1 Configure IM, P2P, streaming media blocking

1. Select **SYSTEM** from the top level administrator console.
2. Click **Control** and select Filter.
3. Set the **Pattern Blocking** radio button to **On**.
4. Select **POLICY** from the top level administrator console.
5. Click Global Group and select Global Group Profile.
6. Move the **Chat, Instant Messaging, Internet Radio, Peer-to-Peer/Filesharing** and **Streaming Media**, from the Pass column to the Block column.
7. Click **Apply**.

2.1.7.2.2 How to test for IM

1. From an IP address in the Global Group range, activate an IM program such as Yahoo! IM or AIM.
2. Attempt to send an instant message to another user. The attempt is blocked.

2.1.7.2.3 How to test for P2P

From an IP address in the Global Group range, attempt to access a P2P site such as Limewire.com. The attempt is blocked.

2.1.7.2.4 How to test for streaming media

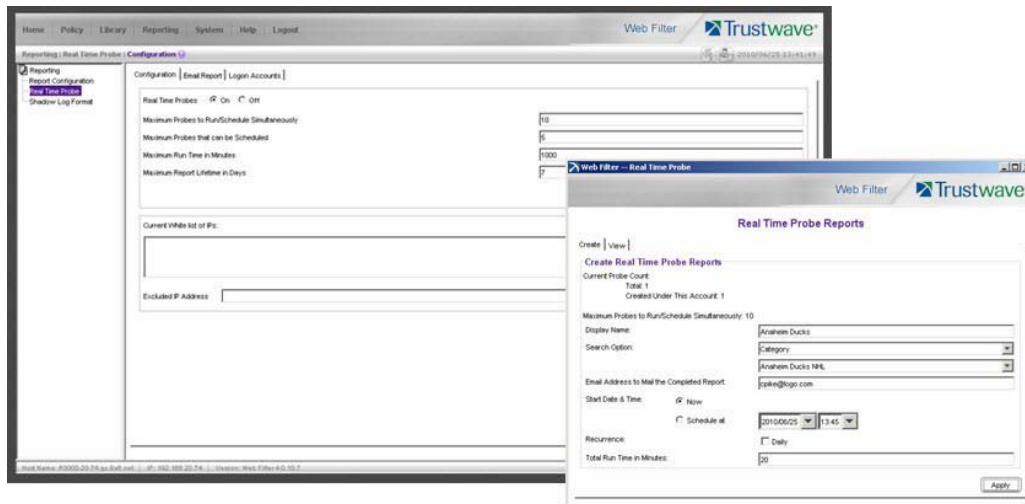
1. From an IP address in the Global Group range, open a streaming media application like Real Audio or Microsoft Media Player.
2. If a stream is not automatically initiated, activate streaming media content. The attempt is blocked.

2.1.8 Real Time Probes and X-Strikes Blocking

2.1.8.1 Real Time Probes feature

Description: Real time probes allow an administrator to monitor an employee's Internet usage in real time to determine if that user is accessing appropriate Internet content. Reports generated by the probe can be emailed for further review. Using Real Time Probes, an administrator can even monitor for malicious code and spyware in real-time to quickly identify workstations that are currently infected.

Figure 24: Real Time Probe setup



2.1.8.1.1 How to configure Real Time Probes

1. Select **REPORTING** from the top level administrator console and choose Real Time Probe.
2. Enable Real Time Probes by selecting **On** and clicking **Save** to apply your setting.
3. Click the link Go to Real Time Probe Reports GUI (lower right corner).
4. Select the **Create** tab do the following:
 - a. Enter a display name for the report (e.g. Spyware Monitoring).
 - b. Select **Category** for the Search option.
 - c. Select a category to be monitored, using the pull-down menu directly below the Search Option (the category choices include custom categories, as well).
 - d. Enter an email address where completed reports will be sent (optional).
 - e. Select **Now** for the Start Date and Time (or set a future date and time).
 - f. Enter the Total Run Time in Minutes you would like the probe to run (e.g. 30).
5. Click **Apply** and **OK** to confirm the creation of the report.

2.1.8.1.2 How to test Real Time Probes

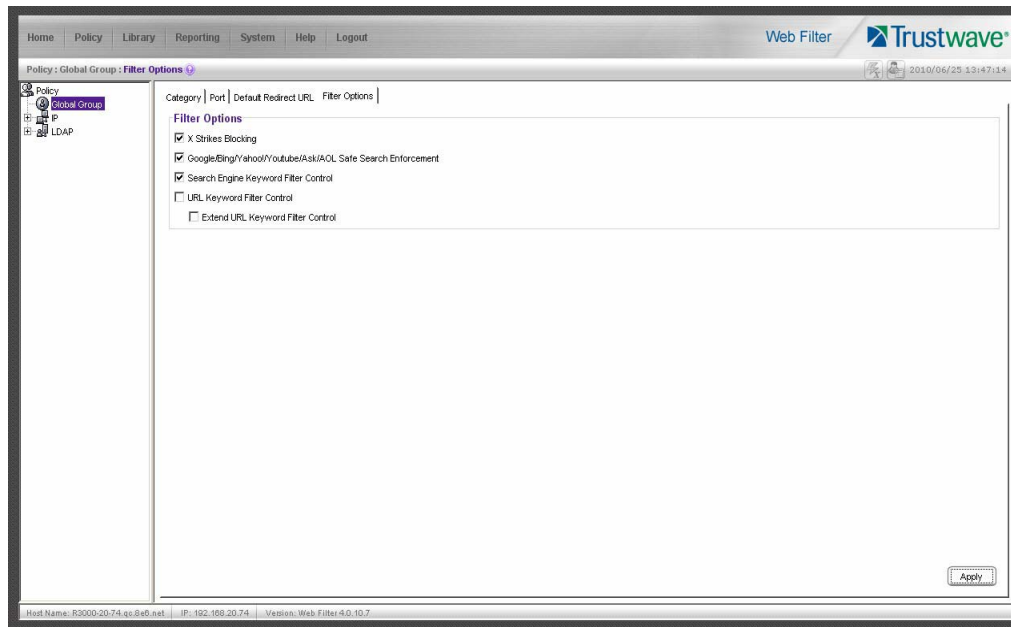
1. Configure a Real Time Probe with the following criteria:

- Maximum Probes to Run/Schedule Simultaneously: 10
 - Maximum Probes that can be Scheduled: 5
 - Maximum Run Time in Minutes: 60
 - Maximum Report Lifetime in Days: 7
 - Display Name: Sports
 - Search Option: Category
 - Category: Sports
 - Start Date & Time: Now
 - Total Run Time in Minutes: 5
2. Click **Apply** and **OK**.
 3. Click the **View** tab to see the probe that you have just created. Its status should show that it's currently running. Highlight the probe and click **View** to see the report run in real time.
 4. Access the Web from an IP address included in the Global Group range.
 5. Begin to access sports-related Web sites and content (e.g., Sports Illustrated and ESPN).
 6. All access to sports-related sites will be identified in this report.

2.1.8.2 X-Strikes feature

Description: The X-Strikes feature is a very powerful administrator tool that enables both the lockdown of users engaged in severe policy violations, as well as, remote notification of the violations, as they occur. X-Strikes is designed to identify and terminate Internet access of users who are frequent violators of policy, e.g. exhibiting multiple attempts to access blocked sites over short periods of time.

Figure 25: X-Strikes feature

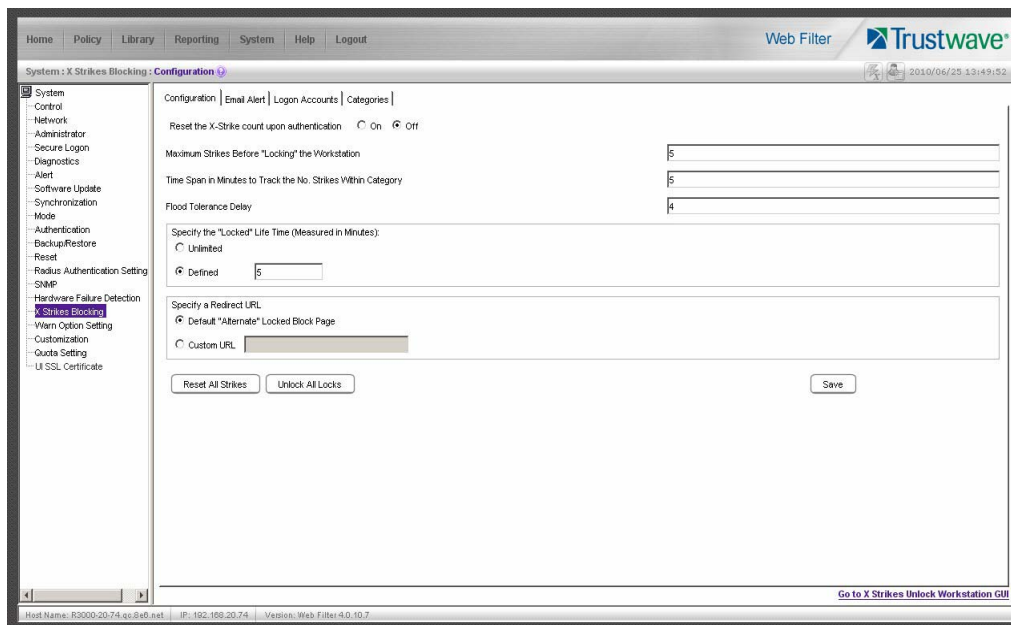


2.1.8.2.1 How to configure the X-Strikes feature

There are two sections of the administrator console that must be accessed to configure the X-Strike feature. First, the feature must be activated in the Global Group options.

1. Select **POLICY** from the top level administrator console.
2. Select Global Group Profile from the Global Group.
3. Select the Filter Options tab in the Global Group window.
4. Select the **X-Strikes Blocking** check box.

Figure 26: X Strikes Blocking

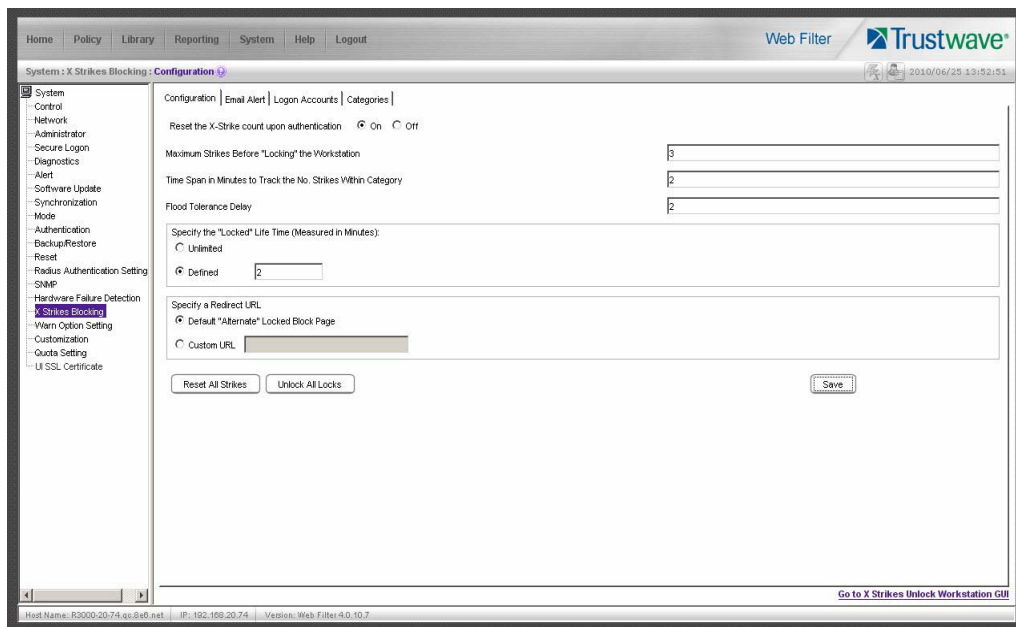


Next, the actual parameters of the X-Strike feature need to be configured.

1. Select **SYSTEM** from the top level administrator console.
2. Click X Strikes Blocking.
3. Make the following settings:
 - a. Select **On** radio button to reset X-Strike Count upon authentication (resets counter for each new user).
 - b. Set **Maximum Strikes Before Locking the Workstation**. The number entered in this field determines how many time a user can attempt to access blocked content before that user is prevented from further Internet access. For example, if the threshold is set at 5, then on the user's fifth attempt to access blocked sites, the computer will be locked down—***if that attempt is made within the time threshold set in step 3b***. The lock disables further access and, instead only displays a block page indicating the reason that access has been blocked.
 - c. Set the **Time Span in Minutes to Track the No. Strikes Within Category**. The number entered in this field determines how long the strikes will be monitored to qualify for a lockdown. For example, if the threshold is set at 5 (minutes) and the Maximum Strikes threshold is set at 5 (attempts), a user who attempts to access five blocked sites being monitored by the X-Strikes feature in a five minute (or less) period of time will be locked out of the Internet and the administrator will be notified. However, if the user attempts to access five blocked sites over the course of an entire day, the standard block page will appear and Internet access will not be locked.

- d. Set the **Flood Tolerance Delay** (in seconds) to determine the maximum delay that will occur before a user who accesses the same URL will receive another block page. If a user receives a block page and attempts to flood the filter through rapid refresh of the page, the X-Strikes feature will not log a strike for every attempt but instead log a strike for each Flood Tolerance Delay threshold that reached. For example, if an employee accesses a blocked site monitored by X-Strikes (which is set at 3 strikes in 1 minute for lockdown), he receives a block page and X-Strikes logs one strike. If the Flood Tolerance Delay is set at 4 seconds, the employee keeps getting block pages, but won't be locked down until 12 seconds has elapsed—no matter how many times he tries to refresh the blocked site.
 - e. **Specify the Locked Life Time (Measured in Minutes)** to determine how long Internet access will be denied.
4. Select the Email Alert tab, and make the following settings:
 - a. In the **Minutes Past Midnight Before Starting Time Interval** field, enter the number of minutes past midnight that a locked work station email alert will first be sent to the specified recipient(s).
 - b. In the **Interval Minutes to Wait Before Sending Alerts** field, enter the number of minutes within the 24-hour period that should elapse between email alerts. For example, by entering 300 in this field and 30 in the previous field, if there are any locked workstations, an email will be sent at 5:30 AM, 10:30 AM, 3:30 PM, 8:30 PM and 12:00 AM (the email alert at midnight fills the gap before the time interval is reset). To check the time(s) the email alert is scheduled to occur, click the Display Sending Time button to open the Daily Schedule pop up window in the (HH:MM:SS) format.
 - c. Click **Save** to save the settings.
 - d. In the **Email Address** field, enter the email address(es) of those who will receive locked workstation alerts.
 - e. Click **Add** to include them in the list.
5. Select the Categories tab.
6. Move the categories from the No Strike category you want monitored to the Strike Categories and vice versa.

Figure 27: X Strikes testing



2.1.8.2.2 How to test X-Strikes

1. Set up X-Strikes with the following settings:

a. Configuration:

- Reset X-Strike Count Upon Authentication: ON
- Maximum Strikes Before Locking the Workstation: 3
- Time Span in Minutes to Track the No. of Strikes Within The Category: 2
- Flood Tolerance Delay: 2
- Specify Locked Life Time: 2
- Specify a Redirect URL: DEFAULT
- Email Alert: enter your email address
- Minutes Past Midnight Before Starting Time Interval: 0
- Interval Minutes to Wait Before Sending Alerts: 1
- Enter an email address to receive alerts; Click Add

b. Categories:

- Strike Categories: Pornography/Adult Content
- No Strike Categories: All others

2. Using an IP within the Global Group range, access www.playboy.com. The site should be blocked.
3. Continue to refresh the page for approximately 6-8 seconds. The workstation's Internet access will be locked and a block page indicating the locked status will appear.
4. After 2 minutes, access will be available again.

5. In approximately 1-2 minutes (the nuances and security settings of the email server will impact the speed of delivery, as well) a notification should be received at the email address noted in the Email Alert field.

3 Security Reporter Evaluation

Security Reporter Evaluation is set up in two sections; the first which explains how to use productivity reports, and the second which explains how to use real time reports.

3.1 Configure and Test Productivity Reports

3.1.1 Understand the most common and useful features

This portion of the Evaluation Guide leads the evaluator through the most common and useful features of the Security Reporter, starting with the elements that should be configured first, then moving on to the usage of the many different types of productivity reports available in the SR. You are directed through the normal path of initial setup, and then led through a standard use case that explains how to investigate a violation of your Internet Acceptable Use Policy.

After stepping through this portion of the Evaluation Guide, you will understand how to set up powerful reports that can be emailed on a regular basis, thus minimizing the effort required for ongoing configuration of the product. In short, by pursuing these exercises, you will discover that the Security Reporter is both easy to use while at the same time best in class in the level of detailed reporting it provides.



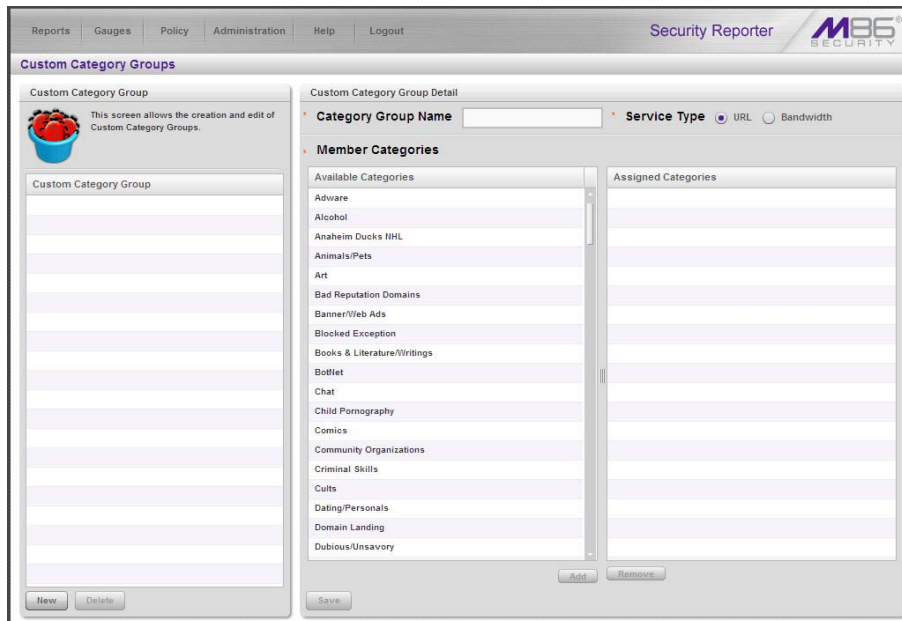
Tip: After the WFR appliance is installed, allow the Security Reporter to run for several days prior to evaluating reports in order to optimize the evaluation experience. This will allow the SR to accumulate multiple days of data and present more meaningful reports. Having performed these preliminary steps, the SR will function properly on day one of the install with some reports showing no data (e.g. "canned" Summary Reports).

3.1.2 Use Custom Category Groups to narrow your search

Prior to running any reports, there are a few recommended configuration steps that create a more customized experience for the evaluator. The first step is to create Custom Category Groups, which are customized groupings from the Trustwave library of more than 100 filter categories. For example, most customers prefer to set up a category group for those categories that are not allowed under their organization's Acceptable Use Policy. Creating such a category group reduces the time it takes to identify violations of this policy.

To create, edit, or delete a Custom Category Group, navigate to Administration | Custom Category Groups to display the Custom Category Groups panel.

Figure 28: Custom Category Groups panel



The Custom Category Groups panel is comprised of two sub-panels used for setting up and maintaining category groups: Custom Category Group, and Custom Category Group Detail.

3.1.2.1 How to add a Custom Category Group

1. At the bottom of the Custom Category Group sub-panel, click **New**.
2. In the Custom Category Group Detail sub-panel, type in the **Category Group Name**.
3. Specify the **Service Type** to use: "URL" or "Bandwidth".
4. Include the following **Member Categories** based on the Service Type selection:
 - URL - Select Available Categories from the list and click **Add** to move the selection(s) to the Assigned Categories list box.
 - Bandwidth - In the **Port Number** field, type in a specific value in the pre-populated field, and/or use the up/down arrow buttons to increment/decrement the current value by one, and then click **Add Port** to move the selection to the Assigned Ports list box.



Note: At least one library category/protocol/port must be selected when creating a gauge. The maximum number of library categories/ports that can be selected/added is 15.

5. Click **Save** to save your settings and to include the name of the group you added in the Custom Category Group list.

3.1.3 Use custom User Groups to narrow your search

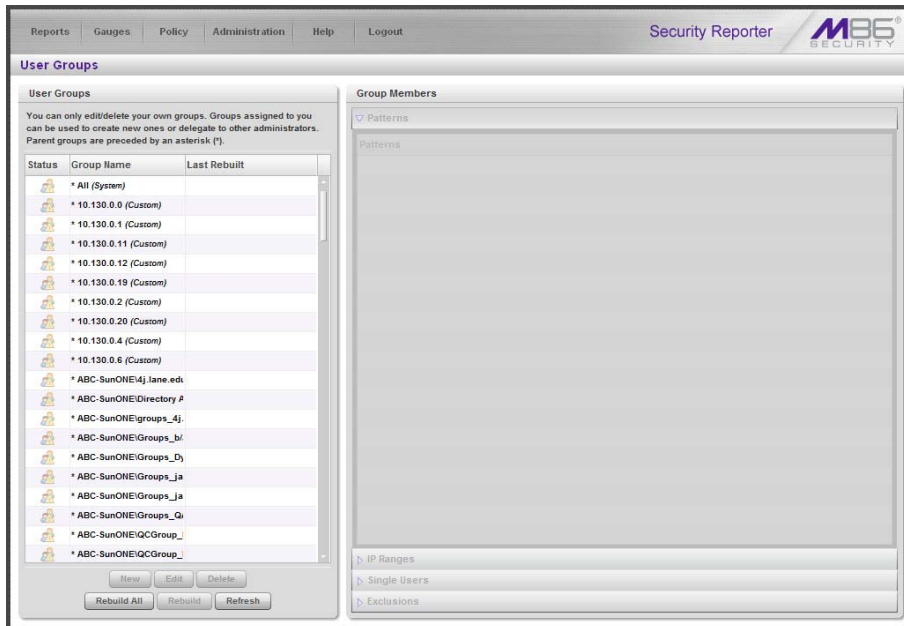
The next step is to create User Groups, which are customized groupings of users that reside on the organization's network. For example, most enterprise customers prefer to set up user groups for each department within the company, and education customers prefer to set up separate user groups for each

classroom or grade level. Creating these user groups reduces the time it takes to identify the source of violations of your organization's Acceptable Use Policy.

3.1.3.1 How to create User Groups

To create, edit, or delete a user group, navigate to Administration | User Groups to display the User Groups panel.

Figure 29: User Groups panel



The User Groups panel is comprised of two sub-panels used for setting up and maintaining user groupings: User Groups, and Group Members.

1. From the User Groups list, select an existing user group to be used as the base group for creating the new user group.
2. Click **New** to display the New User Group panel.

Figure 30: New User Group panel

3. Enter at least three characters for the **Group Name** to be used for the new user group.
4. Click the check box(es) at the top of the panel to activate the pertinent corresponding sub-panel(s) below: **Patterns, IP Ranges, Single Users/Exclude**.
5. After making entries in the pertinent sub-panels—as described in the following sub-sections—click **Save** to save your edits.

3.1.3.1.1 Patterns sub-panel

The Patterns sub-panel is used for adding one or more patterns in order to narrow the list of users to be included in the new group. A pattern consists of a wildcard, or a wildcard plus one or more alphanumeric characters.

1. To add a pattern to the new user group, do one of the following:
 - To add a pattern included in the base group, select the pattern from the Parent Patterns box to display that pattern in the field below.
 - To add a new pattern, enter the pattern in the field beneath the Parent Patterns box. For example: Enter `200.10.100.3%` to include all IP addresses with "200.10.100.3" as part of the IP address.
2. Click **Add Pattern** to include the pattern in the Assigned Patterns list box below.



Tip: Follow steps 1 and 2 above to include additional patterns for the new user group.

3.1.3.1.2 IP Ranges sub-panel

The IP Ranges sub-panel is used for specifying IP ranges to be used by the new group.

Figure 31: Add user group, IP Ranges sub-panel

The screenshot shows the 'New User Group' sub-panel in the Security Reporter application. The 'IP Ranges' tab is selected. The interface is divided into three main sections:

- Patterns:** Contains instructions on using wildcards and escape characters, and lists 'Parent Patterns' and 'Assigned Patterns'.
- IP Ranges:** Contains instructions to assign at least one IP range. It features a 'Parent Ranges' table with columns for 'Starting IP' and 'Ending IP'. Below this are input fields for 'Starting IP' (192.0.0.0) and 'Ending IP' (192.255.255.255), and a 'Calculate IP Range' checkbox which is checked. Below the checkbox are input fields for 'IP Address' (192.168.0.0) and 'Subnet Mask' (255.0.0.0). At the bottom is an 'Assigned Ranges' table with columns for 'Starting IP' and 'Ending IP', containing one row with the values 192.168.0.0 and 255.0.0.0.
- Single Users / Exclude:** Contains instructions on filters and a list of 'Available Users'.

- To add an IP address range, do one of the following:
 - To make a selection from Parent Ranges, click the row in the Parent Ranges box to highlight and select that row, and also to add that Starting IP and Ending IP range in the Starting IP and Ending IP fields below. If necessary, edits can be made to these fields.
 - To add an IP address range without selecting from the Parent Ranges sub-panel:
 - Enter the **Starting IP** address.
 - Enter the **Ending IP** address.
 - To calculate an IP address range:
 - Click the **Calculate IP Range** check box to activate the IP Address and Subnet Mask fields below.
 - Enter the **IP Address**.
 - Enter the **Netmask** which activates the Calculate Range button.
 - Click **Calculate IP Range** to display the Starting IP and Ending IP in the fields above.
- Click **Add IP Range** to include that IP range in the Assigned Ranges list box.

3.1.3.1.3 Single Users/Exclude sub-panel

The Single Users/Exclude sub-panel is used for adding one or more users to the group.



Note: Only users previously selected from the base user group will be included in the Available Users list. A user name preceded by an asterisk (*) indicates an auto-assigned user that can only be removed by adjusting the pattern or IP range for that user's group.

Figure 32: Add user group, Single Users sub-panel

The screenshot shows the 'New User Group' sub-panel in the Security Reporter application. The 'Single Users / Exclude' tab is selected. The interface is divided into three main sections:

- Patterns:** Includes a text area for 'Parent Patterns' and a list for 'Assigned Patterns'. It contains instructions on using wildcards and escape characters.
- IP Ranges:** Includes fields for 'Starting IP' and 'Ending IP', a 'Calculate IP Range' button, and a list for 'Assigned Ranges'.
- Single Users / Exclude:** Includes a text input for 'Available Users Filter', an 'Apply' button, and two lists: 'Available Users' (showing IP addresses like 192.168.20.79) and 'Assigned Users' (currently empty).

To add users to the Assigned Users list, make your selections from the Available Users list. If the Available Users list is long, you can reduce the number of results that display in this list by using the Available Users Filter.

To use the **Available Users Filter**:

1. Enter filter terms to narrow the selection of Available Users. For example: Type in *150%* to only display results matching an IP address that begins with "150".
2. Click **Apply** to display filtered results in the Available Users box.

To make selections from the Available Users box:

1. Select one or more IPs from the list to highlight the record(s).
2. Click **[+] Add** to include the selected user(s) in the Add tab.

3.1.3.2 How to Rebuild a User Group

A user group should be rebuilt if it is edited.

1. To rebuild a user group, select the user group to be rebuilt.
2. Click **Rebuild** to initiate the rebuild process for that user group.
3. After a few minutes, click the **Refresh** button to refresh the display in the panel. Note that the Last Rebuilt column for user group you rebuilt now displays the date and time of the rebuild.

3.1.4 Use Security Reporter to conduct an investigation

Once Custom Category Groups and User Groups have been created, administrators can begin running their first reports. In most cases, administrators will employ the Security Reporter as a forensic tool to

determine if anomalous Internet behavior exists in their organization. In order to facilitate this process, the Security Reporter menu structure is organized to follow the normal process flow of an investigation.

1. First, the administrator is greeted by productivity report content in "**Summary Reports.**"

Additional information can be viewed by navigating to Reports | Dashboard where high-level productivity report information shows data for Blocked Requests and bar graph charts for Top Categories by Requests, Top Security Risks by Requests, Top Blocked Users by Requests, and Top Users by Requests. At a glance, the administrator can see if there is any anomalous behavior that needs investigation.

By viewing either of these types of reports, a specific username might be identified as receiving a large number of blocked requests. Or a high rate of traffic might be identified in the "PornographyAdult Content" category. If something is detected that warrants further investigation, one would then proceed to the "**Drill Down Reports**" section.

2. The next stage of the investigation, Drill Down Reports, lets the administrator probe the multi-dimensional database to target the source of any Internet threat.

For example, if there is unusually high page count in the "Pornography/Adult Content" category, the administrator can drill down into the Category/User section to determine who is viewing this material. Once a specific end user is identified, the administrator can then delve into the detail page view section to see the exact pages that end user has been visiting.

This detailed information provides a wealth of information on the exact time the page was visited, the user's IP address, whether the site was blocked by the Web Filter, how it was blocked (e.g. in URL library, blocked keyword, proxy pattern blocking, etc), and the full-length URL. By viewing this detail, the administrator can obtain an accurate gauge of the user's intent—whether the user repeatedly attempted to go to a forbidden site or whether it was an isolated incident.

3. The last stage of an investigation is to document the long-term activity of a policy violator, since most organizations require more than one or two events to reprimand a user. Once the administrator determines the name of the user and the Web sites visited in the Drill Down Report, the next step is to run a custom report. The administrator can run a specific search of the policy violator for a custom time period by selecting the "**Report Wizard**" option. When generating this type of report, a custom time scope, specific category, and name of a specific end user can be specified.

As an example, the administrator would probably run a custom report for the policy violator by specifying the category "Pornography/Adult Content" and all activity within that category within the last month. The administrator can then save a PDF version of the report for documentation purposes. This custom report provides the necessary forensic information to support any internal reprimand and to protect the organization in the event the incident goes to court.

To summarize, the aforementioned steps were provided to give the user a most-likely use case for the Security Reporter. The next sub-section provides a more in-depth view of how to navigate within each of the main productivity reporting areas of the Security Reporter: Summary Reports, Drill Down Reports, and Custom Reports.

3.1.5 Use Summary Reports for a high level overview

As previously mentioned, Summary Reports provide an administrator an at-a-glance view of any anomalous behavior that warrants an investigation. These “canned reports” contain pre-generated data for a specified period of time (Yesterday, Last Week, Last Month, Week to Yesterday, or Month to Yesterday) for any of the following report topics or entities showing Internet activity:

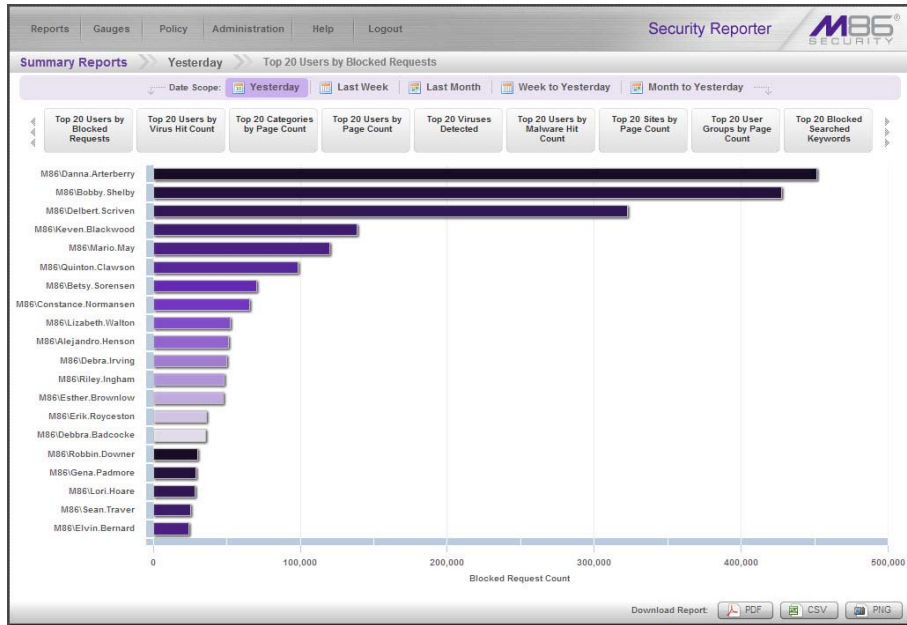
- **Top 20 Users by Blocked Requests** - Bar chart report depicting each top end user’s total Page Count for Blocked and Warn Blocked requests. This report is available if the Block Request Count feature is enabled in the Optional Features screen in the System Configuration administrator console.
- **Top 20 Categories by Page Count** - Bar chart report depicting the total Page Count in the top requested filtering library categories.
- **Top 20 Users by Page Count** - Bar chart report depicting each top end user’s total Page Count.
- **Top 20 Users by Malware by Hit Count** - Bar chart report depicting each top end user’s total “Blocked” and “Permitted” Hit Count from the following categories in the Security, Internet Productivity, and Internet Communication (Instant Messaging) category groups: BotNet, Malicious Code/Virus, Bad Reputation Domains, Spyware, Adware, and IRC.
- **Top 20 Sites by Page Count** - Bar chart report depicting the total Page Count for the most popular sites accessed by end users.
- **Top 20 User Groups by Page Count** - Bar chart report depicting the total Page Count for the top scoring user groups.
- **Top 20 Blocked Searched Keywords** - Bar chart report depicting the total top blocked keyword requests. This report is only available if the Block Searched Keywords Report feature is enabled in the Optional Features screen in the System Configuration administrator console.
- **Total Permitted vs. Blocked Requests** - Pie chart report depicting the total Page Count for all filtering categories Permitted to pass and all filtering categories set up to be Blocked.
- **Category Group Comparison** - Pie chart report depicting the total Page Count in each top scoring filtering category group.
- **Category Comparison** - Pie chart report depicting the total Page Count in each top scoring filtering category.
- **User Group Comparison** - Pie chart report depicting the total Page Count in each top scoring user group.

Once you have obtained an overview of Internet activity using Summary Reports, you can drill down to access more detailed information about specified end user activity.

3.1.5.1 How to generate a Summary Report

1. To generate a Summary Report, go to the navigation panel and click Reports | Summary Reports to display yesterday’s report view showing the Top 20 Users by Blocked Requests.

Figure 33: Yesterday's Top 20 Users by Blocked Requests Report



Note: On a newly installed SR unit, the panel will not show any thumbnail images or bar chart report. If there was no activity for a given report type, the message "No Data to display." displays in the panel.



Tip: Click the left arrows or right arrows at the edges of the dashboard to display thumbnail images that are currently hidden. Mouse over each bar in the bar graph to view the name of graph entry and number of requests for that entry.

2. Click a **Date Scope** tab corresponding to the time period to be included in the report: "Yesterday", "Last Week", "Last Month", "Week to Yesterday", or "Month to Yesterday".
3. Click one of the report type thumbnails beneath the Date Scope to display that report view.
4. To see details for the generated Summary Report view, at the bottom of the report view, click a **Download Report** option for PDF, CSV, or PNG to generate a report in the specified file format (.pdf, .csv, or .png).

Figure 34: Sample Bar Chart Summary Report in the PDF format

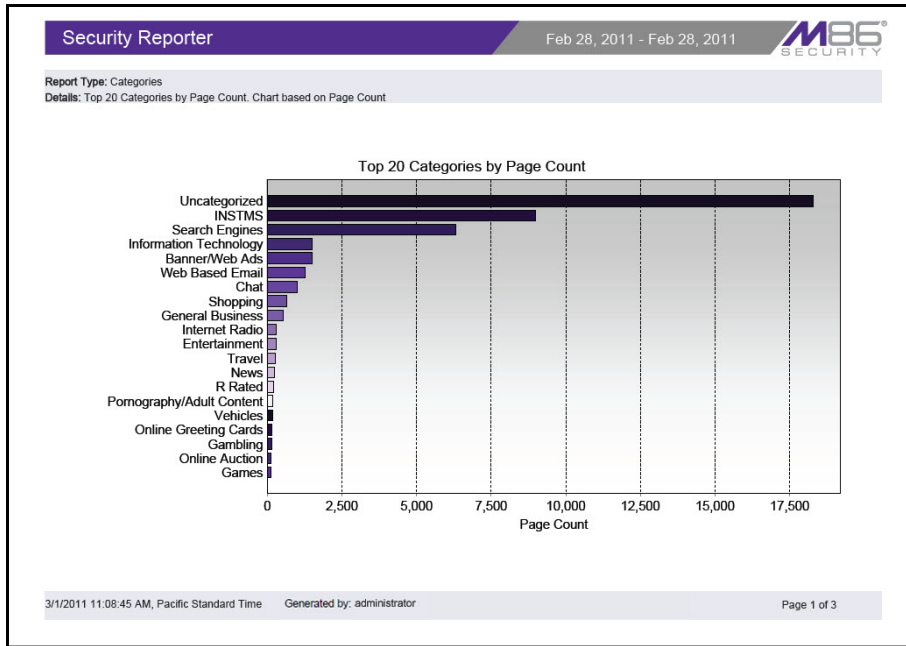
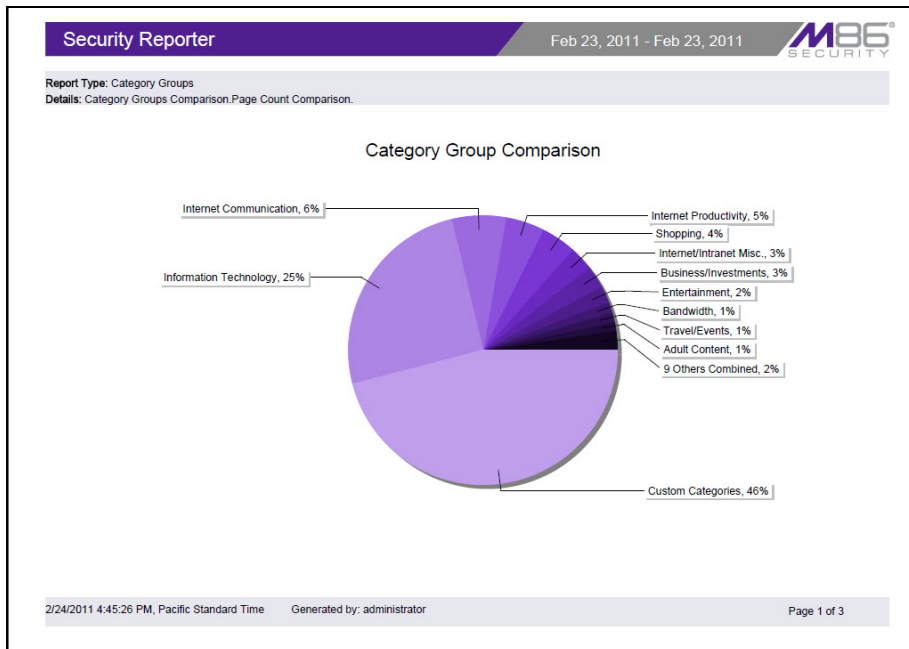


Figure 35: Sample Pie Chart Summary Report in the PDF format



The header of the generated report includes the date range, Report Type, and Details criteria.

The footer of the report includes the date and time the report was generated (using the M/D/YYYY, H:M:S AM/PM format), administrator login ID (Generated by), and Page number and page range.

The body of the first page of the report includes the following information:

- Bar chart - Name of category, username, username path, URL or site IP address, user group name, or blocked user request, and corresponding bar graph. Beneath the bar graph are count indicators and a label describing the type of Count used in the report.
- Pie chart - Color-coded pie graph showing a maximum of 15 categories or user groups. Any categories or user groups with page counts totalling less than one percent are grouped together under the "Others Combined" label.

The body of the pages following the first page of the bar or pie chart report includes the following information:

- Top 20 Users by Blocked Requests report - User NAME and corresponding BLOCKED REQUEST COUNT—which includes Blocked and Warn Blocked requests. Total Records and Total Number of Blocked Requests for this Date Scope display at the end of the report.
- Top 20 Blocked Searched Keywords report - Blocked Keywords and corresponding Blocked Count. A Grand Total of Blocked Count displays at the end of the report.
- All other reports - Count columns and corresponding totals for all reports. Grand Total and Count display at the end of the report.

3.1.5.2 How to export a Summary Report

From the open PDF file, the Summary Report can be exported in some of the following ways:

- Print the report - Click the print icon to open the Print dialog box, and proceed with standard print procedures.
- Save the report - Navigate to File | Save (Page) As... to open the Save As dialog box, and proceed with standard save procedures.

3.1.6 Use Drill Down Reports for an investigation

In the event that Summary Reports in the Security Reporter dashboard reveal abnormal activity, the next step in the investigation would be to drill down into the particular category or user information.

This section provides information about "drill down" reports that let you query the database to access more detailed information about end user Internet activity. The following types of reports can be generated:

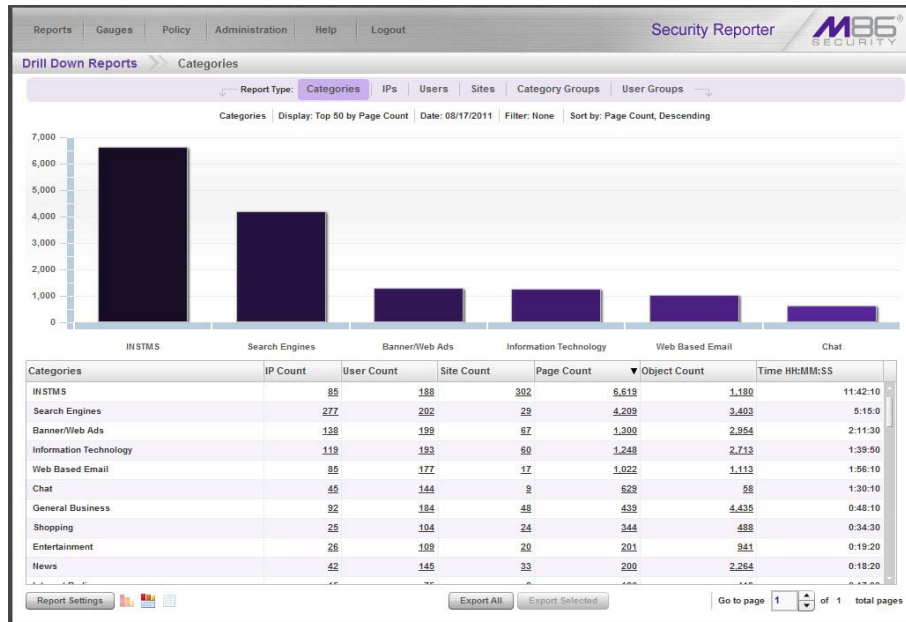
- **Categories** - Includes data in each filter category that was set up for monitoring user activity.
- **IPs** - Includes Internet activity by user IP address.
- **Users** - Includes Internet activity by username.
- **Sites** - Includes activity on Web sites users accessed.
- **Category Groups** - Includes activity by Category Groups.
- **User Groups** - Includes activity by User Groups.

Once you have generated a drill down report view, you can customize your view, save the view, export the view, and/or schedule the report to run at a designated time.

3.1.6.1 How to generate a Summary Drill Down Report

1. To generate a summary Drill Down Report, go to the navigation panel and click Reports | Drill Down Reports, and choose the report type to be generated. The first menu selection is "Categories"; making this selection displays today's Categories report view by Page Count.

Figure 36: Sample Drill Down Categories Report (summary report)



For each report type, by default the top portion of the report view includes tabs for all productivity Report Types (Categories, IPs, Users, Sites, Category Groups, and User Groups). The following information displays beneath this row of tabs: report type, Display criteria, Date, Filter criteria, and Sort by criteria. Beneath this row, a bar chart depicts the first six records for the current report type.



Note: Mousing over a bar in the chart displays the name of the record along with the total count used in that record.

Beneath the bar chart is a table containing rows of records. Columns of pertinent statistics display for each record.

3. Use the tools at the bottom portion of the report view panel to modify the current report view, creating the desired drill down view.



Note: See 'Summary Drill Down Report navigation' for information on using the reporting elements described in this sub-section.

4. The drill down view can be exported, saved, and/or scheduled to run at a specified time.

3.1.6.2 Summary Drill Down Report navigation

Continuing from the last section, this section is designed to help the administrator learn how to navigate within the Summary Drill Down Report. The Drill Down report is unique in terms of the seemingly endless

ways data can be displayed, but it is important to understand all of the functions within this tool in order to generate meaningful reports.

3.1.6.2.1 Count columns and links

In a summary drill down report view, Count columns (Category Count, IP Count, User Count, Site Count, Page Count, Object Count) display after the column containing the record name. Clicking a specific link in a record's Count column gives more in-depth analysis on a given record displayed in the current view.

- **Category Count** - Displays the number of categories a user has visited, or the number of categories included within a given site. It is possible for a site to be listed in more than one category, so even if a user has visited only one site, this column may count the user's visit in two or three categories.
- **IP Count** - Displays the number of sites or categories visited by the IP address for a user's machines.
- **User Count** - Displays the number of individuals who have visited a specific site or category.
- **Site Count** - Displays the number of sites a user has visited, or the number of sites in a category. This figure is based on the root name of the site. For example, if a user visits www.espn.com, www.msn.com, and www.fox-sports.com, that user will have visited three pages. If that same user additionally visits www.espn.com/scores, the total number of sites visited would still count as three—and not as four—because the latter page is on the original ESPN site that was already counted.
- **Page Count** - Displays the total number of pages visited. A user may visit only one site, but visit 20 pages on that site. If a user visits a page with pop-up ads, these items would add to the page count. If a page has banner ads that link to other pages, these items also would factor into the page count. In categories that use a lot of pop-up ads—porn, gambling, and other related sites—the page count usually exceeds the number of objects per page.

By clicking the link in this column, the detail report view displays data for all pages accessed, including hyperlinks to those pages. In the detail report view, you have the option to exclude Information columns for Date, Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, Search String, and URL by de-selecting the corresponding check boxes via the Column Visibility option.

- **Object Count** - Displays the number of objects on a Web page. All images, graphics, multimedia items, and text items count as objects. The number of objects on a page is generally higher than the number of pages a user visits.

However, if an advertisement or banner ad (an object on the page) is actually a page from another site, this item would not be classified as an object but as a page, since it comes from a different server.

By clicking the link in this column, the detail report view displays data for all objects accessed, including hyperlinks to those objects. In the detail report view, you have the option to include Information columns for Date, Category, User IP, User name, Site, Filter Action, Content Type, Content criteria, Search String, and URL by deselecting the corresponding check boxes via the Column Visibility option.



Note: If "Pages only" was specified in the Log Import Settings sub-panel of the Optional Features screen in the System Configuration user interface, **all** records of objects accessed by end users will be lost for the time period in which this option was enabled. Even if there were objects accessed by end users during that time period, zeroes ("0") will display in the Object Count column in the report. See the Optional Features sub-section of the System Configuration Section for information about Log Import Settings sub-panel options.

3.1.6.2.2 Time column

In a summary drill down report view, the **Time HH:MM:SS** column provides additional information about a record, displaying the amount of time a user spent at a given site. Each page detected by a user's machine adds to the count. If a browser window is opened to a certain page and left there for an extended time period, and that page is refreshed by either the user or a banner ad, the counter starts again and continues as long as Web activity is detected. If that Web page contains an active banner ad that refreshes the page every 10 to 30 seconds, a user could show an incredibly high page count and many minutes, even though only one page was opened by that user.

3.1.6.2.3 Column sorting tips

To sort summary report view records in ascending/descending order by a specified column, click that column's header: Category Count, IP Count, User Count, Site Count, Page Count, Object Count, or Time HH:MM:SS.

Click the same column header again to sort records for that column in the reverse order.

Click another column header to sort records by that specified column.

3.1.6.2.4 Record exportation

In a summary drill down report view, all records are selected for exportation by default. Clicking **Export All** opens the Export pop-up window in which you specify criteria for the report to be generated and distributed.

To select only specific records to export, click the first column of selected record rows in the table, and then click **Export Selected** to open the Export pop-up window.

3.1.6.2.5 Navigation tips

- Report view breadcrumb trail links - When generating a report view and modifying that report view to create another report view, a trail of breadcrumb links remain in the row beneath the navigation toolbar. Clicking a link returns you to that prior report view.
- Page navigation - At the bottom right of the panel, the **Go to page** field displays:

Go to page of 2 total pages

If more than one page of records displays for the total pages returned, enter a page number within that range to navigate to that page of records, or use the up/down arrow(s) to specify the page you want displayed.

3.1.6.3 How to generate a Detail Drill Down Report

By using the Summary Drill Down Report, the administrator should have narrowed the investigation to a specific category (e.g. "Pornography/Adult Content") and a specific user name. The next step is to drill down into the detailed URL information to confirm the exact pages visited by the suspected policy violator.

To generate a detail drill down report, select the record and click the link in the "Page Count" column of the Summary Drill Down Report.

Figure 37: Detail Drill Down Report view

Date	Category	User IP	User	Site	Filter Action	Content ...	Content	S...	URL
8/17/2011 12:0...	Web Base...	142.117.174.59	testDomainUse...	getemail sympa...	Allowed	URL	http://getemail.sympat...		http://getemail.sympatico.ca/GetTips?Page...
8/17/2011 12:0...	Web Base...	142.124.185.31	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=809e3d35a...
8/17/2011 12:0...	Web Base...	142.183.188.97	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=8a4d16f0...
8/17/2011 12:0...	Web Base...	142.117.27.93	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=38588eddf...
8/17/2011 12:0...	Web Base...	142.127.133.54	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind7a...
8/17/2011 12:0...	Web Base...	142.183.123.32	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind7a...
8/17/2011 12:0...	Web Base...	142.180.18.248	testDomainUse...	msn.com	Allowed	URL	http://by1046.bay104...		http://by1046.bay104.hotmail.msn.com/cgi...
8/17/2011 12:0...	Web Base...	142.122.218.85	testDomainUse...	yahoo.com	Allowed	Wildcard	http://MAIL.yahoo.co...		http://520.mail.yahoo.com/vmllogin?rand=...
8/17/2011 12:0...	Web Base...	142.180.197.91	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind7a...
8/17/2011 12:0...	Web Base...	142.127.135.79	testDomainUse...	142.182.19.28	Allowed	URL	https://mail.google.co...		https://142.182.19.28
8/17/2011 12:0...	Web Base...	142.117.159.70	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/test2at...
8/17/2011 12:0...	Web Base...	142.127.135.79	testDomainUse...	142.182.19.28	Allowed	URL	https://mail.google.co...		https://142.182.19.28
8/17/2011 12:0...	Web Base...	142.127.135.79	testDomainUse...	142.182.19.28	Allowed	URL	https://mail.google.co...		https://142.182.19.28
8/17/2011 12:0...	Web Base...	172.26.144.117	testDomainUse...	yahoo.com	Allowed	Wildcard	http://MAIL.yahoo.co...		http://mail.yahoo.com/
8/17/2011 12:0...	Web Base...	142.113.116.70	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=20da607eb...
8/17/2011 12:0...	Web Base...	142.117.159.70	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=7f6b47ea6...
8/17/2011 12:0...	Web Base...	142.122.66.24	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind7a...
8/17/2011 12:0...	Web Base...	142.127.133.54	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=8eaf55c...
8/17/2011 12:0...	Web Base...	172.26.150.72	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind7a...
8/17/2011 12:0...	Web Base...	142.117.159.70	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/?ik=7f6b47ea6...
8/17/2011 12:0...	Web Base...	142.117.159.70	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind7a...
8/17/2011 12:0...	Web Base...	142.122.84.68	testDomainUse...	google.com	Allowed	URL	http://mail.google.com/		http://mail.google.com/mail/channel/bind7a...

3.1.6.3.1 Detail Drill Down Report navigation

Report type columns - In the detail report view, by default all Page/Object Detail column(s) display. Any of these columns can be hidden from view by clicking the **Column Visibility** button at the bottom of the panel to open the Column Visibility pop-up window, and de-selecting the check box corresponding to that column:



- **Date** - Displays the date in the M/D/YYYY H:M:S AM/PM format
- **Category** - Displays the category name (e.g. "Alcohol").
- **User IP** - Displays the IP address of the user's machine (e.g. "200.10.101.80").
- **User** - Displays any of the following information: username, user IP address, or the path and username (e.g. "logo\admin\jsmith").
- **Site** - Displays the URL the user attempted to access (e.g. "coors.com").

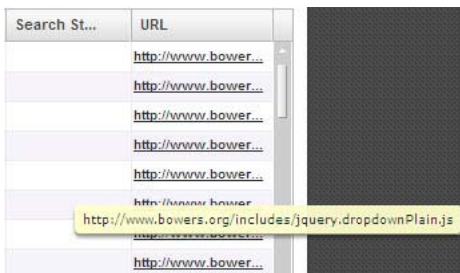
- **Filter Action** - Displays the type of filter action used by the Web Filter in creating the record: "Allowed", "Blocked", "Warn Blocked" (for the first warning page that displayed for the end user), "Warn Allowed" (for any subsequent warning page that displayed for the end user), "Quota Blocked" (if a quota blocked the end user), "X-Strike", or "N/A" if the filter action was unclassified at the time the log file was created.
- **Content Type** - Displays the method used by the Web Filter in creating the record: "Search KW" (Search Engine Keyword), "URL KW" (URL Keyword), "URL", "Wildcard", "Https High" (HTTPS Filtering Level set at High), "X-strike" (X Strikes Blocking), "Pattern" (Proxy Pattern Blocking), "File Type", "Https Medium" (HTTPS Filtering Level set at Medium), or "N/A" if the content was unclassified at the time the log file was created.
- **Content** - Displays criteria used for determining the categorization of the record, or "N/A" if unclassified.
- **Search String** - Displays the full search string the end user typed into a search engine text box in search sites such as Google, Bing, Yahoo!, MSN, AOL, Ask.com, YouTube.com, and MySpace.com—if the Search Engine Reporting option is enabled in the Optional Features screen of the System Configuration administrator console user interface.
- **URL** - Displays the link for the page/object accessed by the end user.

3.1.6.3.2 Detail Drill Down Report exercise

For the purpose of this evaluation, follow these steps to witness how the Security Reporter is best in class in terms of the extent of detailed page and object information it provides.

1. Select a specific user by Category - If not already completed, click the "Page Count" column link for any record in the Summary Drill Down Report.
2. Sort by "Filter Action" column - Clicking the "Filter Action" column header will sort all records by the type of filter action—whether the event was blocked, allowed or warned. Blocked searches will be highlighted in red font for easier detection.
3. Full URL review - The full length URL of every Internet search by the users is listed in the "URL" column of the detail page information.

To view record data that displays truncated in a column, mouse over the column to view the entire string of data in the column for a given record:



Click the URL link to launch the actual Web site viewed by the user to verify the content that was accessed.

4. Sort by "Content Type" - Sort by the column labeled "Content Type" by clicking that column header. This will sort all records by the search type filtered on the Web Filter. For example, "URL" indicates a page request was blocked or allowed based on the status of that URL in the Web Filter category library and "Search KW" indicates a user typed in a prohibited word into a search engine text box. One of Trustwave's differentiators is "Proxy Pattern Blocking," which will show up in the "Content Type" section if an Internet proxy site was blocked by Trustwave's proprietary proxy signature detection.

After reviewing a suspected policy violator's Internet activity in the Detail Drill Down Report, the administrator will have firm evidence on the user's *intent*, which is critical forensic information to have in the event the investigation moves to the disciplinary phase.

5. Sort by "Search String" - Sort by the column labeled "Search String" by clicking that column header. This will sort all records alphabetically for results that include search string information. Search string content includes the actual text typed into a search engine text box on popular search engine sites such as Google, Bing, Yahoo!, YouTube, Ask.com, and MSN. For example, if the end user typed in "recipes for chicken breast" in a search engine request, that entire string will appear in this column, not simply the blocked keywords within the request. This depth of detail helps clarify the intent of the end user, which helps tremendously in investigations.

In the next section, this guide will go through the final step in a typical investigation—creating a custom report for a specific user via the productivity Report Wizard.

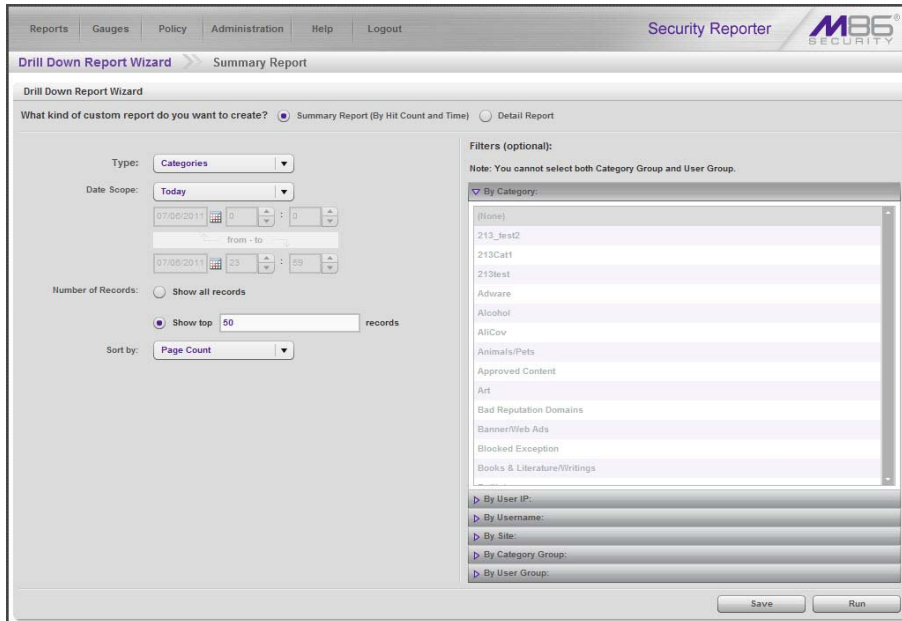
3.1.7 Create a custom report for a specific user

After reviewing the detail drill down report, if the administrator is confident that an individual has violated the Internet Acceptable Use Policy (AUP), the most common step to take next is to run a custom report for this specific individual that covers a greater time period. While there are several ways to accomplish this in the Security Reporter, this guide will focus on the most commonly used method—the productivity **Report Wizard**.

3.1.7.1 How to use the Report Wizard for a single user report

The Report Wizard option provides an intuitive setup process for generating custom reports for one time use, or for recurrence at scheduled time periods. The productivity "Report Wizard" option is available by navigating to Reports | Drill Down Reports | Report Wizard.

Figure 38: Report Wizard panel for summary reports

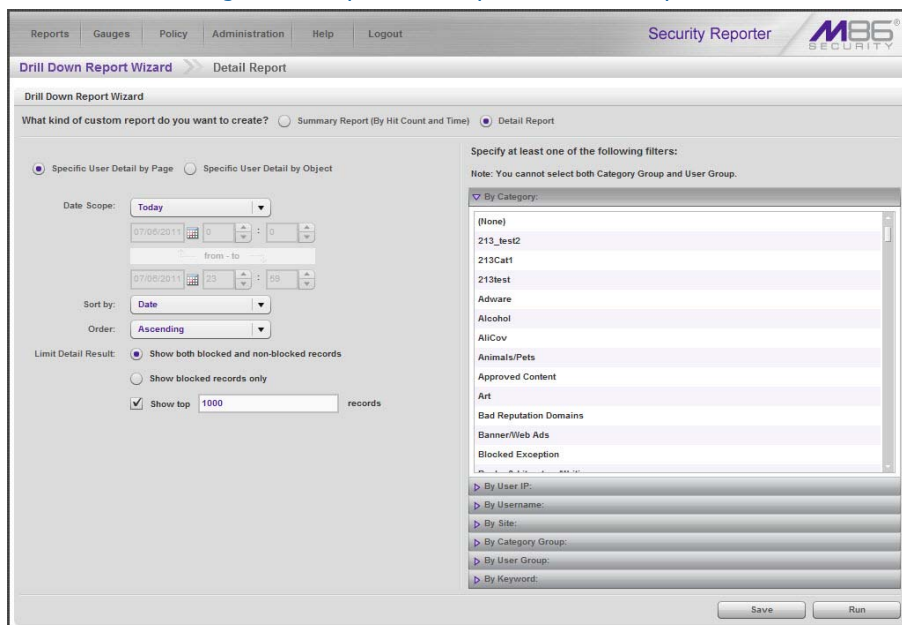


3.1.7.1.1 Create either a Summary Report or a Detail Report

Select one of two available custom productivity report options:

- **Summary Report (By Hit Count and Time)** - This report provides a synopsis of specified end user Internet activity by hit count and time for a designated period.
- **Detail Report** - This report provides information about end user Web page or Web object access for a specified time period.

Figure 39: Report Wizard panel for detail reports



3.1.7.1.2 Specify the Report Type

- Summary report - Make a choice for the **Type** of report to be generated; for this exercise, choose "Categories" or "Sites".

In this exercise, narrow your results for the specified user by choosing the **Filters (optional)** accordion for "By User IP" or "By Username", as described in the next section.

- Detail report:
 - a. Choose the type of detail report to use in the query:
 - **Specific User Detail by Page** - Includes viewed page results
 - **Specific User Detail by Object** - Includes viewed object results
 - b. **Specify at least one of the following filters** in the accordions at right to narrow your search—for this exercise, "By User IP" or "By Username"—as described in the next section.

3.1.7.1.3 Specify Filters

For this exercise, choose either of these filters:

- **By User IP** - If selecting this filter, enter the end user IP address for filtering your results—using the '%' wildcard to return multiple IP addresses—and then click **Search** to display query results in the list box below.
- **By Username** - If selecting this filter, enter the end user name to filter your results—using the '%' wildcard to return multiple usernames—and then click **Search** to display query results in the list box below.

For a detail report, select the username and click the right arrow (>) to move the username into the Added user names list box.

3.1.7.1.4 Specify Other Report Components

Specify criteria for the remaining components to be used in the report:

- **Date Scope** - Choose the date scope to be included in the results.



Note: For detail reports, if more than one username or if any keyword is entered in this panel, the following Date Scope choices are the only choices available: "Yesterday" (default), "Previous 7 Days", selections for Previous 6, 5, 4, 3, or 2 Days, and "Daily".

- **Number of Records** - For a summary report, specify the number of records to be returned in the results.
- **Sort by** - Select column by which the results will be sorted and displayed in the report.
- **Order** - For a detail report, indicate whether results will be sorted in "Ascending" or "Descending" order.
- **Limit Detail Result** - For a detail report, specify the number of records to be returned in the results, and if these records will only include records of blocked end user queries, or also records of non-blocked end user queries.

3.1.7.1.5 Specify when to Generate the Report

Indicate the next step in the wizard by selecting one of two choices that specify when the report will be generated:

- **Run** - Click this button to generate and view the drill down report now in the specified report view format.
- **Save** - Click this button to go to the Save Report panel where you save your report criteria now but generate your report later.

3.1.7.1.6 Save the Report

1. Click the **Save** button to display the Basic Options tab of the Drill Down Reports | Report Wizard | Save Report panel.

Figure 40: Drill Down Report Wizard's Save Report panel Basic Options tab

2. In the **Save Name** field, enter a name for the report. This name will display in the Reports | Saved Reports list box.



Tip: The Copy (Ctrl+C) and Paste (Ctrl+V) functions can be used in the fields in this screen.

3. In the **Description** field, enter the report description.
4. Specify **Email** criteria:
 - **To** and **Subject**, and optional fields for Body, Cc, and Bcc.
 - **Hide Unidentified IPs** check box is de-selected by default if the "Hide Unidentified IPs" check box is de-selected in the Default Report Settings panel.
 - **Output Type** - Choose either "Email As Attachment", or "Email As Link".

- **Format** - Choose from available output format selections in the pull-down menu.



Note: Any selected filter options display to the right.

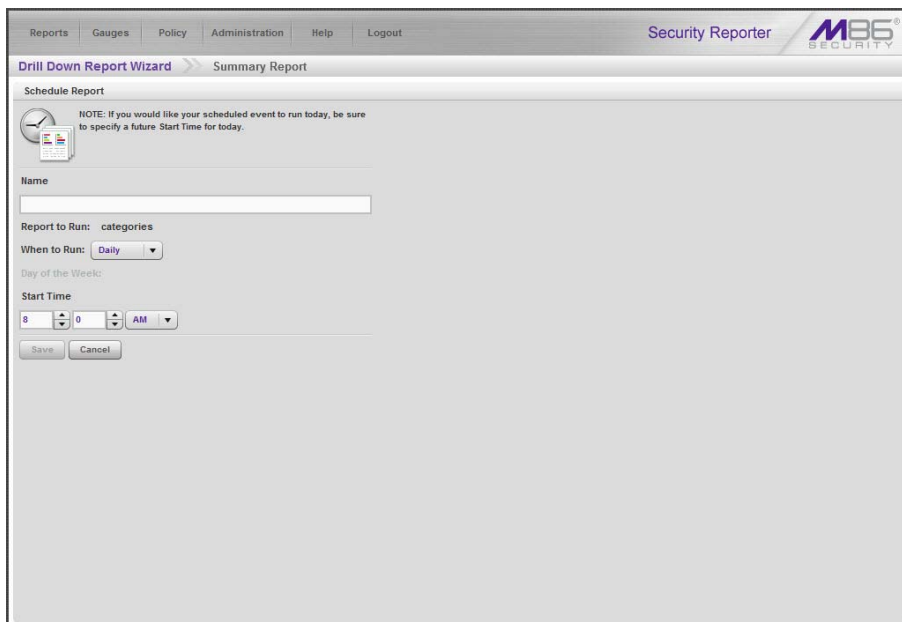
5. Click the Advanced Options tab for additional options:

- **Group By** - Available selections are based on the type of report specified.
- For summary reports, at the **For multi-level Group By reports only** field, if a selection was made in the Group By field, specify the top count option to be used in the **Number of Records** and **Sort By** fields.
- For a summary report, **For pie and bar charts only**, the activated **Generate Using** field lets you select the count column sort option.
- For detail reports, specify any of the following options:
 - **Detailed Info** - Uncheck any check box corresponding to a column that should not be included in the report.
 - **Limit Detail Result** - Indicate the maximum number of records to be included in the report, and whether these records will only include blocked end user queries, or also records of non-blocked end user queries.

6. Specify the next—or final—step in the wizard by selecting one of three choices:

- **Save and Schedule** - Click this button to save your entries and to go to the Schedule Report panel where you set up a schedule for running the report.

Figure 41: Drill Down Report Wizard's Schedule Report panel



- a. Enter a **Name** for the **Report to Run**.
- b. Select the frequency **When to Run** from the pull-down menu (Daily, Weekly, or Monthly). If Weekly, specify the **Day of the Week** from the pull-down menu (Sunday - Saturday).

If Monthly, specify the **Day of the Month** from the pull-down menu (1 - 31).

c. Select the **Start Time** for the report: 1 - 12 for the hour, 0 - 59 for the minutes, and AM or PM.



Note: The default Start Time is 8:00 AM. If you wish to run a report today and this time has already passed, be sure to select a future time.

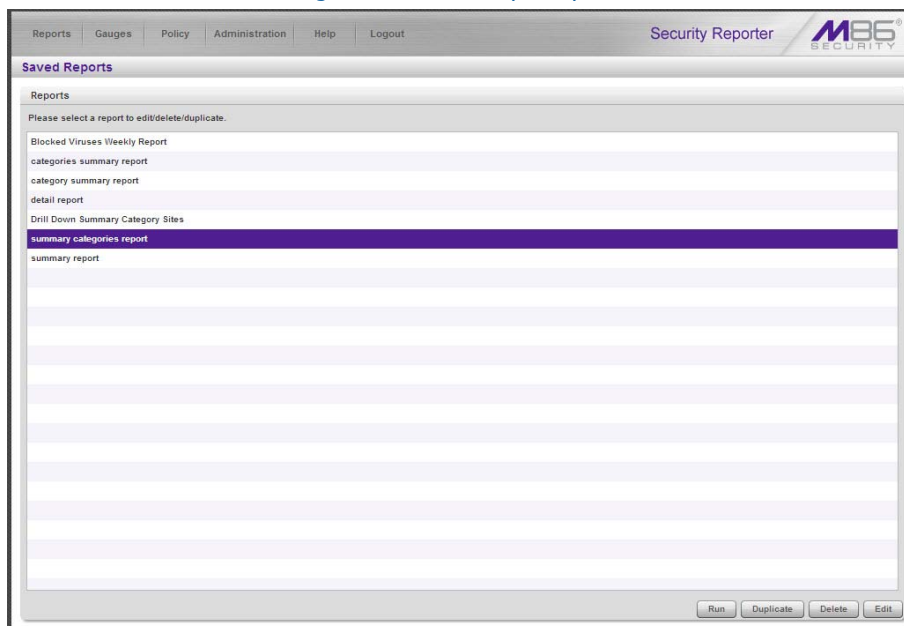
d. Click **Save** to save your report schedule settings and to go to the Report Schedule panel where the report is now included in the list.



Tip: Click **Cancel** to save the report and to return to the Report Wizard panel without scheduling a time for running the report.

- **Save and Email** - Click this button to save your entries and to email the generated report to the designated recipient(s). After the report is emailed, the Saved Reports panel displays if you need to run this report again or another report.

Figure 42: Saved Reports panel



- **Save Only** - Click this button to save your entries and to go to the Saved Reports panel where you can delete, edit, or run this report or another report.

3.1.8 Export Summary Drill Down Reports

For this exercise, you will learn how to export a customized Summary Drill Down Report.

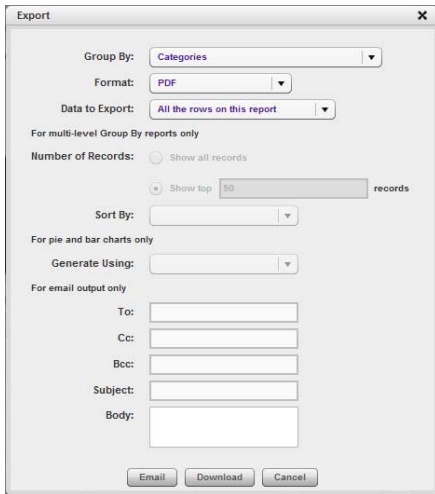
3.1.8.1 How to export selected records

3.1.8.1.1 Select records to be exported

To only include specific records in the summary drill down report, click the first column of each row containing the selected record while simultaneously depressing the Ctrl key in the keyboard.

3.1.8.1.2 Specify Data to Export

1. Click the **Export Selected** button to open the Export pop-up box:



2. At the **Data to Export** field pull-down menu, specify the amount of data to be exported. For this exercise, choose "Only selected rows on this page".

3.1.8.1.3 Export data via Email or PDF Download option

1. Make selections and/or entries in all available fields in the Export pop-up box.
2. Click the **Email** or **Download** button to close this pop-up box and to export the data—via email or to your workstation—in the specified file format.
 - Email option - The email option for exporting reports lets you electronically send the report in the specified file format to designated personnel.



Caution: If using a spam filter on your mail server, email messages or attachments might not be delivered if these messages contain keywords that are set up to be blocked. Consult with the administrator of the mail server for work around solutions between the spam filter and mail server.

- a. In the Export pop-up box, enter the following information:
 - To** field - Type in the email address of each intended report recipient, separating each address by a comma (,) and a space.
 - Subject** field (optional) - Type in a brief description about the report.
 - Cc** field (optional) - Type in the email address of each intended recipient of a carbon copy of this message, separating each address by a comma (,) and a space.
 - Bcc** field (optional) - Type in the email address of each intended recipient of a blind carbon copy of this message, separating each address by a comma (,) and a space.
 - Body** field (optional) - Type in text pertaining to the report.

- b. Click **Email** to send the report to the designated recipient(s).



Caution: Large reports might not be sent due to email size restrictions on your mail server. The maximum size of an email message is often two or three MB. Please consult your mail server administrator for more information about email size restrictions.

- View and print options - The view and print options for exporting reports let you view/print the report in the specified file format. The view option lets you make any necessary adjustments to your report file settings prior to printing the report. To print the report, you must have a printer configured for your workstation.

In the Export pop-up box, click the **Download** button to generate and download the report in the specified file format.



Note: Reports generated in the format for MS-DOS Text, Comma-Delimited Text, or Excel (Chinese or English) will display a single row of text for each record. Reports generated in all other formats (PDF, Rich Text Format, HTML) will display any lengthy string of text wrapped around below.

3.1.8.2 Sample report file formats

The following report file formats are available for emailing and viewing: "MS-DOS Text", "PDF", "Rich Text Format", "HTML", "Comma-Delimited Text", "Excel (Chinese)", "Excel (English)".



Note: Trustwave recommends using the PDF and HTML file formats over other file format selections—in particular for detail reports—since these files display and print in a format that is easiest to read. Lengthy text in PDF, HTML, and Rich Text Format files wraps around within the column so all text is captured without displaying truncated.

Comma-Delimited Text and Excel report columns may display with truncated text, but an entire column can be viewed by manipulating the column width in the generated report file. These reports can then be printed at a smaller percentage than normal size in order to accommodate all text.

For MS-DOS Text reports, text may display truncated—in particular for lengthy usernames and URLs in detail reports—but an entire column can be viewed by scrolling to the right. Since there is no way to manipulate text in the generated report file, the printed report may display with truncated text. However, the maximum amount of text can be captured by printing the report in the landscape format.

3.1.8.2.1 PDF

This is a sample of the Category Groups report in the PDF format, saved with a .pdf file extension.

Figure 43: Category Groups report, PDF format

Security Reporter		Oct 20, 2011 - Oct 20, 2011						M86 [®] SECURITY	
Category Groups									
Top 50 Category Groups by Page Count sorted by Page Count, descending									
Category Groups	Category Count	IP Count	User Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
Information Technology	2	35	203	14	116	136	0:14:0	252	0
Travel/Events	1	4	21	4	29	119	0:2:40	148	0
Internet Communication	3	8	34	6	27	14	0:4:30	41	0
Internet Productivity	1	14	79	10	18	178	0:3:0	196	0
Business/Investments	3	15	77	6	17	372	0:2:50	389	0
Shopping	2	2	16	2	16	0	0:2:40	16	0
Entertainment	3	6	34	6	11	63	0:1:50	74	0
Adult Content	2	3	12	2	8	11	0:1:20	19	0
News/Reports	2	6	30	5	1	104	0:0:10	105	0
Bandwidth	2	3	13	2	0	17	0:0:0	17	0
Education	1	1	8	1	0	28	0:0:0	28	0
Society/Lifestyles	1	2	16	2	0	20	0:0:0	20	0
Games	1	1	8	1	0	32	0:0:0	32	0
Streaming Media	1	1	4	1	0	8	0:0:0	8	0
Grand Total	25	101	555	62	243	1,102	0:33:0	1,345	0
Count:	14								

10/20/2011 8:31:27 AM, Pacific Daylight Time Generated by: wizard Filter: None Page 1 of 1

Examples of other report formats are provided in the Trustwave WFR Administrator Guide.

3.1.9 Summary Drill Down Reporting tools

The Security Reporter has a variety of different reporting options. In a fashion similar to the specific user report creation process, administrators can also create custom reports from any Drill Down Report view. These reports can be set up to be automatically emailed to the administrator on a regular basis in a variety of formats (e.g. PDF, Excel, etc.).

3.1.9.1 How to use other Summary Drill Down Report tools

3.1.9.1.1 Limit Detail Result

1. At the bottom left of the report view, hover over **Report Settings** and select **Limit Detail Result** to open the Limit Detail Result pop-up box:

2. Indicate the limit for the set of records to be returned by selecting the appropriate radio button:
 - **Show all records** - Click this radio button to include all records returned by the report query.
 - **Show first 'X' records** - Click this radio button to only include the first set of records returned by the report query.

3. Indicate the number of records to be included in a set by making an entry in the blank field, represented here by the 'X'.
4. Click **Apply** to apply your settings in the current report view and to close this pop-up box.

3.1.9.1.2 Report fields

- **Type field** - The Type field is used for specifying the report type for the summary report to be generated.

At the **Type** field, make a selection from the pull-down menu for one of the available report types: "Categories", "IPs", "Users", "Sites", "Category Groups", "User Groups", and the current report format displayed.

- **Date Scope and Date fields** - The Date Scope field is used for specifying the period of time to be included in the generated report view. Depending on the scope selected, the From Date and To Date fields are used in conjunction with this field.

At the **Date Scope** field, make a selection from the pull down menu for the time sub-panel you wish to use in your query: "Today", "Month to Date", "Monthly", "Year to Date", "Daily", "Yesterday", "Month to Yesterday", "Year to Yesterday", "Last Week", "Last Weekend", "Current Week", "Last Month". Reports can be run for any data saved in the SR's memory.

- **Today** - This option generates the report view for today only, if logs from the Web Filter have been received and processed.
- **Month to Date** - This option generates the report view for the range of days that includes the first day of the current month through today.
- **Monthly** - Selecting this option activates the **from** and **to** date fields where you specify the date range using the calendar icons.
- **Year to Date** - This option generates the report view for the range of days that includes the first day of the current year through today.
- **Daily** - Selecting this option activates the **from** and **to** date fields where you specify the date range using the calendar icons. The generated report view includes data for the specified days only, if the data for these days are stored on the SR.
- **Yesterday** - This option generates the report view for yesterday only.
- **Month to Yesterday** - This option generates the report view for the range of days that includes the first day of the current month through yesterday.
- **Year to Yesterday** - This option generates the report view for the range of days that includes the first day of the current year through yesterday.
- **Last Week** - This option generates the report view for all days in the past week, beginning with Sunday and ending with Saturday.
- **Last Weekend** - This option generates the report view for the past Saturday and Sunday.

- **Current Week** - This option generates the report view for today and all previous days in the current week, beginning with Sunday and ending with Saturday.
- **Last Month** - This option generates the report view for all days within the past month.
- **Number of Records fields** - The Number of Records fields are used for specifying the number of records from the query you wish to include in the summary drill down report view, and how these records will be sorted.

In the **Number of Records** field, indicate whether the report view should "Show all records" or "Show top 'x' records". If the latter selection is made, the value that displays in this field may have come from the Default Report Settings panel and can be modified.

- **Filter and Filter String fields** - The filter fields are used for narrowing results that display in the current summary drill down report view.

At the **Filter** field, make a selection from the pull-down menu for the filter term to be used: "None", "Contains", "Starts with", "Ends with".

The **Filter String** field displays greyed-out if "None" was selected at the Filter field. If any other selection was made at that field, enter text in this field corresponding to the type of filter term to be used.

- **Sort By and Limit summary result to fields** - The sort fields are used for specifying the report view column by which the generated report will be sorted.

At the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: "Name of 'x'", "Category Count", "IP Count", "User Count", "Site Count", "Page Count", "Object Count", "Time", "Hit Count".

If the "Name of 'x'" option is selected, the **Limit summary result to** field displays. Make a selection from the pull-down menu for one of the available choices for which the summary report results will be limited: "Top Category Count", "Top IP Count", "Top User Count", "Top Site Count", "Top Page Count", "Top Object Count", "Top Time", "Top Hit Count".

- **Group By field** - The Group By field is used for indicating the manner in which records will display for the specified report view when exported.

Choose from the available report selections at the **Group By** pull-down menu. Based on the current report view displayed, the selections in this menu might include the main report type such as "Sites", double-combination report types such as "Users/Sites", triple-combination report types such as "User/Category/IPs", or pie or bar charts.

- **Format field** - The Format field is used for specifying the manner in which text from the report view will be outputted.

At the **Format** pull-down menu, choose the format for the report: "MS-DOS Text", "PDF", "Rich Text Format", "HTML", "Comma-Delimited Text", "Excel (Chinese)", and "Excel (English)".

- **For multi-level Group By reports only** - The Number of Records and Sort By fields are used when exporting multi-combination summary drill down reports and are deactivated by default.

- **Number of Records field** - The Number of Records field is used for specifying the number of records that will display for the selected sort option. By default, this field displays greyed-out and becomes activated when a different Group By option is selected.

In the activated **Number of Records** field, indicate whether to "Show all records" or "Show top 'x' records".

- **Sort By field** - The Sort By field is used for specifying the report view column by which the generated report will be sorted.

At the **Sort By** field, make a selection from the pull-down menu for one of the available sort options: "Category Count", "IP Count", "User Count", "Site Count", "Page Count", "Object Count", "Time", "Hit Count".

- For pie and bar charts only:

- **Generate Using field** - The Generate Using field is used when exporting a drill down Categories, Category Group, or User Group pie chart or bar chart report, and determines by which column the report will be sorted. By default, the field displays greyed-out and becomes activated when a pie or bar chart report is selected from the Group By pull-down menu.

At the activated **Generate Using** field, make a selection from the pull-down menu for the sort option to be used: "Category Count", "IP Count", "User Count", "Site Count", "Page Count", "Object Count", "Time", "Hit Count".

- **Output Type field** - The Output Type field is used for specifying how the generated report will be sent to the recipient(s).

At the **Output Type** field, choose either "Email As Attachment", or "Email As Link".

- **Hide Unidentified IPs check box** - The Hide Unidentified IPs check box is used for specifying whether or not IP addresses of workstations that are not assigned to a designated end user will be included in reports. This check box is deselected by default if the check box by this same name was de-selected in the Default Report Settings panel.

To change the selection in this field, click the **Hide Unidentified IPs** check box to remove—or add—a check mark in the check box. By entering a check mark in this check box, activity on machines not assigned to specific end users will not be included in report views. Changing this selection will not affect the setting previously saved in the Default Report Settings panel.

- **Email / For email output only fields** - Email fields are used for entering email criteria pertinent to the report to be sent to the designated addressee(s).

Specify the following in the **Email** or **For Email output only** fields:

- **To** - Enter the email address of each intended report recipient, separating each address by a comma (,) and a space.
- **Subject** - Type in a brief description about the report.
- **Cc** (optional) - Enter the email address of each intended recipient of a carbon copy of this message, separating each address by a comma (,) and a space.

- **Bcc** (optional) - Enter the email address of each intended recipient of a blind carbon copy of this message, separating each address by a comma (,) and a space.
- **Body** - Type in text pertaining to the report.

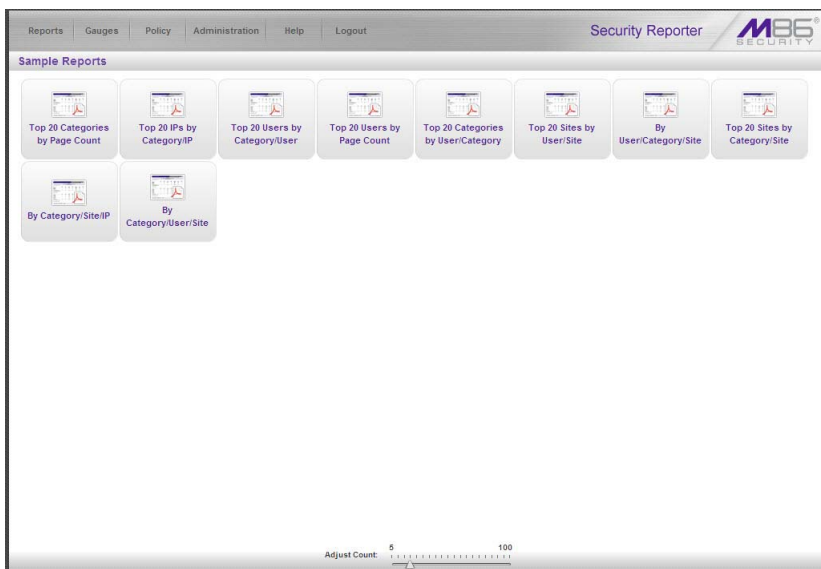
3.1.10 Commonly used reports

Though this portion of the Evaluation Guide is primarily designed to lead the evaluator through the process of an investigation using common productivity reports, there are many other useful features to explore in Security Reporter productivity reports. Below is a summary of some of the other custom reports an administrator can create and have automatically emailed on a regular basis in order to be kept up to date on Internet threats arising from within the organization.

Trustwave has created 10 different sample report formats to help first time users understand the various types of reports available in the Security Reporter. For purposes of this Evaluation Guide, only three of the 10 are described in detail below. A description of all other sample reports is available in the SR Productivity Reports Section of the WFR Administrator Guide.

3.1.10.1 How to generate a Sample Report

1. From the Reports menu, choose **Sample Reports**:



2. Click one of the following thumbnails to open a separate browser window containing the generated Sample Report in the PDF format:

- **Top 20 Categories by Page Count**
- **Top 20 IPs by Category/IP**
- **Top 20 Users by Category/User**
- **Top 20 Users by Page Count**
- **Top 20 Categories by User/Category**

- **Top 20 Sites by User/Site**
- **By User/Category/Site**
- **Top 20 Sites by Category/Site**
- **By Category/Site/IP**
- **By Category/User/Site**

3. From the open PDF file, the Sample Report can be printed or saved.
4. Click the "X" in the upper right corner of the report window to close it.

3.1.10.1.1 Report format

The report header contains the following information: "Security Reporter" and date range for today's date; report name; description for that report type, including the sort order and **Page Count, descending**.

The body of the report contains rows of records and is comprised of one or more sections.

For each record, end user statistics display in columns such as: Category Count, IP Count, Site Count, Page Count, Object Count, Time (HH:MM:SS), Hit Count, and Blocked Hits.

Total counts display at the end of each section.

The Grand Total and total Count for all sections display at the end of the report.

The footer on each page contains the following information: today's date (M/D/YYYY format), time (HH:MM:SS AM/PM), and time zone in which the report was generated; **Generated by:** manager's login ID; **Filter: None;** **Page** number and page range.

3.1.10.1.2 Examples of available Sample Reports

- Sample Report 1: "Top 20 Users by Category/User" - This report shows the top 20 users for each of the categories in the Trustwave library. This is a useful tool to quickly scan for excessive use of any category.

Figure 44: Sample Category/Users report

Security Reporter		Oct 20, 2011 - Oct 20, 2011				M86 [®] SECURITY	
Category/Users							
All Categories sorted by Page Count, descending							
Top 20 Users by Page Count in each Categories table							
Category:INSTMS							
Users	IP Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
testDomain\User35575	1	13	14	0	0:2:10	14	0
testDomain\User94579	1	13	14	0	0:2:10	14	0
testDomain\User85458	1	13	14	0	0:2:10	14	0
testDomain\User73417	1	13	14	0	0:2:10	14	0
testDomain\User63178	1	13	14	0	0:2:10	14	0
testDomain\User77805	1	13	14	0	0:2:10	14	0
testDomain\User06086	1	13	14	0	0:2:10	14	0
testDomain\User27036	1	13	14	0	0:2:10	14	0
testDomain\User14045	1	13	14	0	0:2:10	14	0
testDomain\User85960	1	13	14	0	0:2:10	14	0
testDomain\User57336	1	6	7	0	0:1:0	7	0
testDomain\User63449	1	6	7	0	0:1:0	7	0
testDomain\User22681	1	6	7	0	0:1:0	7	0
testDomain\User43953	1	6	7	0	0:1:0	7	0
testDomain\User07417	1	6	7	0	0:1:0	7	0
testDomain\User04703	1	6	7	0	0:1:0	7	0
testDomain\User48497	1	3	4	0	0:0:30	4	0
testDomain\User66515	1	3	4	0	0:0:30	4	0
testDomain\User70653	1	3	4	0	0:0:30	4	0
testDomain\User21216	1	3	4	0	0:0:30	4	0
Total for INSTMS							
User Count: 20 sorted by Page Count, descending							
	20	178	198	0	0:29:40	198	0
Category:Search Engines							
Users	IP Count	Site Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
10/20/2011 11:17:34 AM, Pacific Daylight Time Generated by: wizard Filter: None Page 1 of 19							

- Sample Report 2: "Top 20 Sites by User/Site" - This report will document the top 20 sites visited for every user in the organization. This is a useful tool in monitoring the high level Web activity of users, and can help fine-tune sites the administrator allows users to access.

Figure 45: Sample User/Sites report

Security Reporter		Oct 20, 2011 - Oct 20, 2011				M86 [®] SECURITY	
User/Sites							
All Users sorted by Page Count, descending							
Top 20 Sites by Page Count in each Users table							
User:testDomain\User63178							
Sites	Category Count	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
142.180.3.173	1	1	2	0	0:0:10	2	0
142.183.222.56	1	1	1	0	0:0:10	1	0
142.180.188.33	1	1	1	0	0:0:10	1	0
172.19.1.53	1	1	1	0	0:0:10	1	0
142.182.118.79	1	1	1	0	0:0:10	1	0
142.117.8.48	1	1	1	0	0:0:10	1	0
142.182.51.242	1	1	1	0	0:0:10	1	0
142.127.169.106	1	1	1	0	0:0:10	1	0
161.216.141.146	1	1	1	0	0:0:10	1	0
142.113.79.130	1	1	1	0	0:0:10	1	0
172.26.224.36	1	1	1	0	0:0:10	1	0
142.182.30.42	1	1	1	0	0:0:10	1	0
142.127.133.54	1	1	1	0	0:0:10	1	0
Total for testDomain\User63178							
Site Count: 13 sorted by Page Count, descending							
	13	13	14	0	0:2:10	14	0
User:testDomain\User85960							
Sites	Category Count	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
142.180.3.173	1	1	2	0	0:0:10	2	0
142.183.222.56	1	1	1	0	0:0:10	1	0
142.180.188.33	1	1	1	0	0:0:10	1	0
172.19.1.53	1	1	1	0	0:0:10	1	0
142.182.118.79	1	1	1	0	0:0:10	1	0
142.117.8.48	1	1	1	0	0:0:10	1	0
142.182.51.242	1	1	1	0	0:0:10	1	0
10/20/2011 11:27:36 AM, Pacific Daylight Time Generated by: wizard Filter: None Page 1 of 228							

- **Sample Report 3: "By Category/User/Site"** - This is an example of a triple break report that shows all activity on the network, broken out by category, then user, and then site. This is a useful report if the administrator is looking for an all-encompassing view of Internet activity within the organization. However, please note that this is usually a very lengthy report since it captures all user information by site.

Figure 46: Sample Category/User/Sites report

Security Reporter		Oct 20, 2011 - Oct 20, 2011		M86 [®] SECURITY		
Category/User/Sites						
All Categories sorted by Page Count, descending						
All Sites in each Users table						
Category:INSTMS						
User:testDomain\User01196						
Sites	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
207.46.110.14	1	0	1	0:0:0	1	0
Total for testDomain\User01196						
Site Count: 1 sorted by Page Count, descending						
Category:INSTMS						
User:testDomain\User01909						
Sites	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
aim.com	1	0	1	0:0:0	1	0
Total for testDomain\User01909						
Site Count: 1 sorted by Page Count, descending						
Category:INSTMS						
User:testDomain\User03106						
Sites	IP Count	Page Count	Object Count	Time (HH:MM:SS)	Hit Count	Blocked Hits
aim.com	1	0	1	0:0:0	1	0
Total for testDomain\User03106						
Site Count: 1 sorted by Page Count, descending						
Category:INSTMS						
10/20/2011 11:30:09 AM, Pacific Daylight Time Generated by: wizard Filter: None Page 1 of 300						

3.2 Configure and Test Real Time Reports

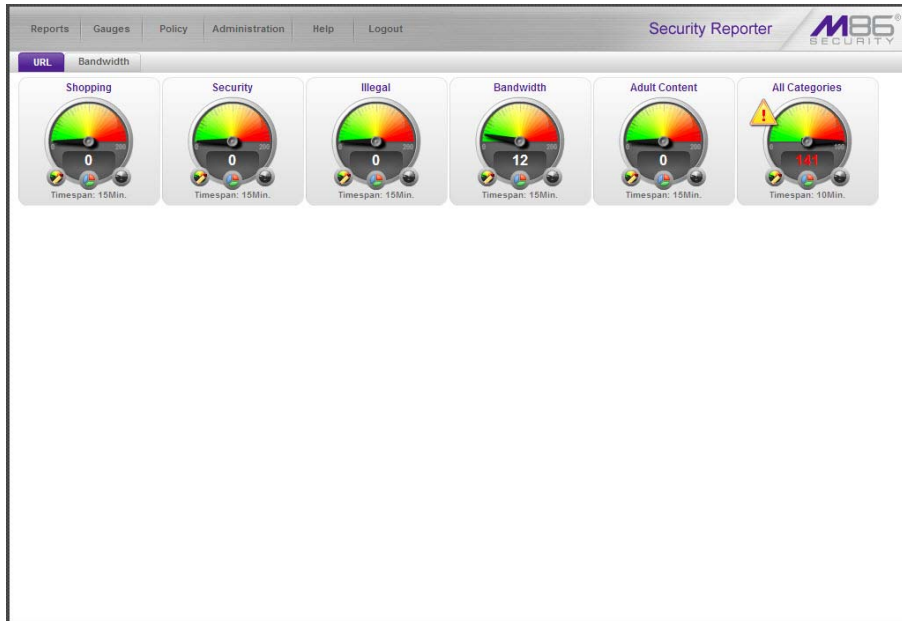
3.2.1 Understand the most common and useful features

In this portion of the Evaluation Guide, you will learn how to read URL Dashboard gauges that target areas on your network that could potentially endanger its security and/or usurp most of its bandwidth, and how to identify users who are violating your organization's policies and prevent them from continuing to pursue such activities.

3.2.2 Monitor URL gauges

When clicking **Gauges** in the navigation toolbar, the URL Dashboard displays.

Figure 47: URL dashboard with URL gauges



Note: The bandwidth gauges dashboard is displayed by clicking the Bandwidth button to the right of the URL button above the dashboard. The bandwidth gauges dashboard shows you end user activity for bandwidth protocols set up to be monitored by the Security Reporter. More about bandwidth gauges is described later in this section of the Evaluation Guide.

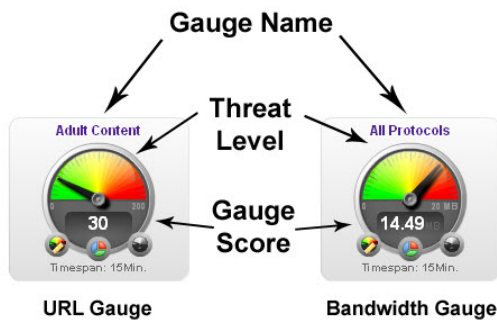
Each URL gauge represented in the Dashboard is comprised of library categories and monitors a targeted user group’s access of URLs in a specified library category.

3.2.2.1 How to drill down into a URL gauge

This exercise will step you through the manual monitoring of users in real time via the URL gauges Dashboard. Note that this is simply one of many ways to use SR to monitor insider threats. There is also a robust automated alert component that does not require the system administrator to be monitoring gauges in order to be notified of a violation in process.

3.2.2.1.1 How to read a URL gauge

The graphic and sub-sections below describe how to read gauges on the URL gauges Dashboard:



- Gauge Name - The gauge name is the customized name of the gauge created by the administrator. SR has five default sample gauges that correspond to five of Trustwave’s super-categories: Shopping, Security, Illegal, Bandwidth and Adult Content. Administrators can create their own gauges as well as delete the default gauges.

- Gauge Score - The gauge score is the large number in the center of the gauge that is based upon the number of URL page hits (see NOTES below) that occur in this specific category in a given period of time.



Note: In addition to page hits, SR also counts “blocked object” hits. For reference, “pages hits” are files that typically end in .html and represent a main page view. “Object hits” are files that typically end in .gif or .jpg and represent image files.

To streamline your task, SR does not track a score for “non-blocked objects,” since these gauges are designed to provide a clear picture of how many times a user has requested a page, and objects are images hosted within a page. SR includes blocked object data to cover instances in which harmful images are hosted on a non-harmful site.

- Timespan - Each gauge monitors events in real time for a window of time between one and 60 minutes. This timespan is customizable by the administrator. For example, if a gauge is set for 15 minutes, that gauge will indicate the number of page hits for the last 15 minutes of time. For example, if the current time is 12:00, the gauge score will reflect all activity from 11:45 to 12:00. Once the time is 12:01, the gauge will reflect all activity from 11:46 to 12:01.
- Threat Level - The colored threat level indicates the current state of threat based on the customizable ceiling created by the administrator. For example, if the administrator creates a gauge with a threshold of 100, when the score reaches 67 the gauge dial will move into the red threat level section, the score will turn red, and a yellow warning triangle symbol will appear and begin to flash.



These gauges are designed to provide an intuitive reminder when a specific category gauge is experiencing abnormal levels of activity so the administrator can react quickly.

3.2.2.1.2 Identify the source of a gauge’s activity

Each gauge is comprised of one or more gauge components—derived from library categories in the Web Filter. Sometimes end user activity in a single component is responsible for driving a gauge’s score.

To identify the source of a gauge’s activity, from the URL dashboard you can either click the gauge or right-click the gauge and then select “View Gauge Ranking”:

Performing either of the two aforementioned actions on the gauge will open the Gauge Ranking panel showing a list of all end users affecting this gauge’s components, and all affected components in this gauge.

Figure 48: Gauge Ranking panel

Username	Bandwidth	Liability	Others	Productivity	Security	Total
GA\franklin	0	0	7	10	109	126
192.168.30.87	0	0	7	10	74	91
192.168.30.80	0	0	27	40	14	81
192.168.30.85	30	0	16	6	0	52
192.168.30.88	0	0	1	2	14	17
192.168.30.74	0	0	16	0	0	16
192.168.30.84	0	0	0	0	8	8
Novell3020\HUSEE	0	0	0	6	2	7

If a single component is affecting the entire gauge, you can investigate activity in that component by drilling down into the component with the highest score.

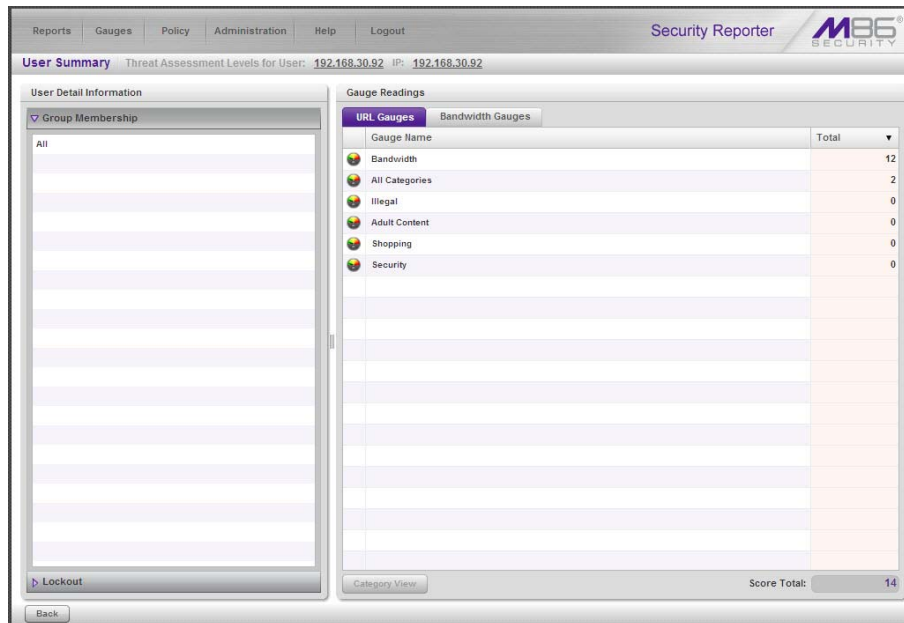
3.2.2.1.3 View a list of Threats the end user accessed

In the Gauge Ranking panel, click the highest score in a column for a component; this action displays the Category View User panel showing a list of all Categories accessed by the selected end user for the gauge component.

Figure 49: List of Threats accessed by the user for a gauge

Categories	Total
Banner/Web Ads	55
Web Based Email	28
Image Servers & Image Search Engines	12
Free Hosts	4
Yahoo IM	2

Figure 51: User Summary panel



A list of groups to which the user belongs displays to the left, and a list of gauges displays to the right, showing the user's score for each gauge.

To drill down and view activity in any gauge the user affected, select the gauge, and then click the Category View button at the bottom of the panel to display the Category View User panel.



Note: There is also a way to automatically lock out the user that will be demonstrated later in this document.

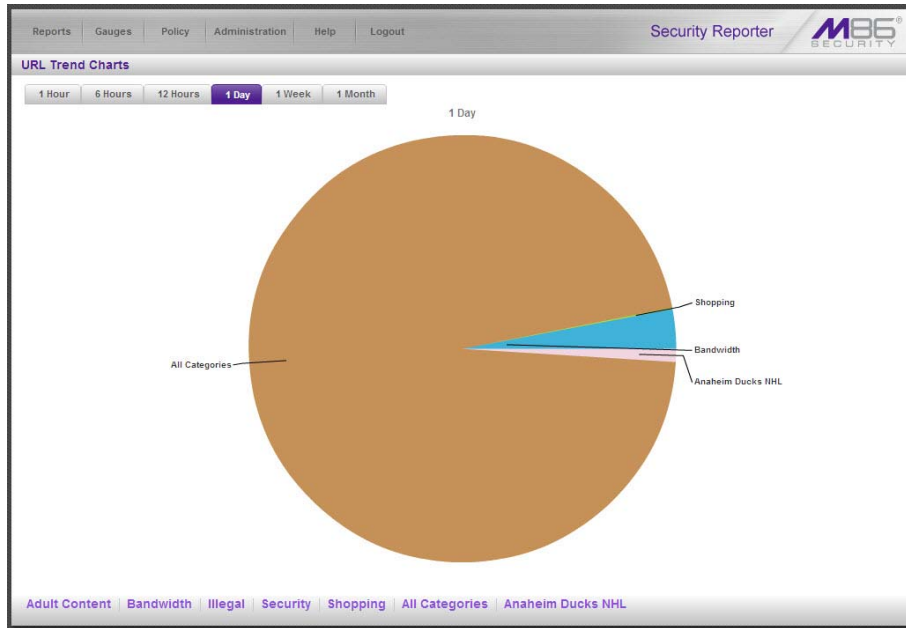
3.2.2.2 How to view URL Trend Reports

SR lets you generate historical trend reports that show activity by URL threats for a specified time period. These trend reports are helpful for monitoring improvement of activity in a certain library category as well as providing a good tool for setting appropriate thresholds for each URL gauge.

3.2.2.2.1 View overall activity in URL gauges

Navigate to Reports | URL Trend Charts to display the URL Trend Charts panel.

Figure 52: URL Trend Charts panel



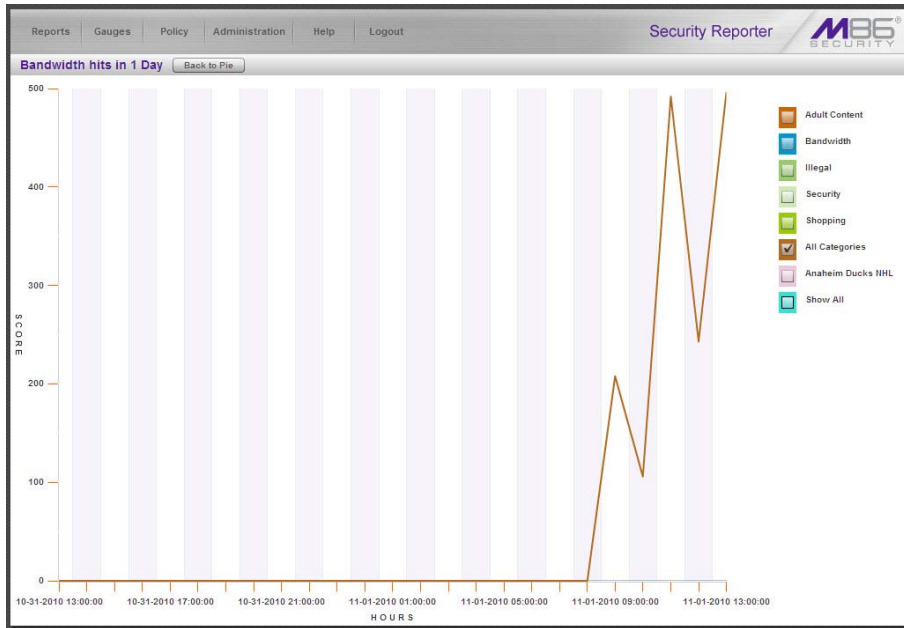
The pie trend chart is divided into pie slices named for each gauge in which there was activity. The size of each slice is determined by the amount of activity in that gauge for the designated time period, in comparison to activity in all other URL gauges during that same time period. All activity is translated into a percentage figure, with the total activity for all slices equaling 100 percent.

You can change the time span represented in the trend chart by clicking one of five other tabs at the top of the chart. Choices range from the last hour to the last month of data.

3.2.2.2.2 View a line chart for a single URL gauge

To uncover more information about activity in a particular gauge, click the pie slice for that gauge to view a line chart depicting that gauge's activity within the specified time period.

Figure 53: Activity for a specified gauge



Tip: You can also go to the bottom of the pie chart and click a tab for a gauge to access the line chart for that gauge within the specified time period.

The score and minutes in which activity occurred display, represented by a line graph. The chart can be modified by clicking check boxes to the right to include lines in the chart depicting activity in other gauges.

3.2.2.3 How to view a pie chart for a URL gauge

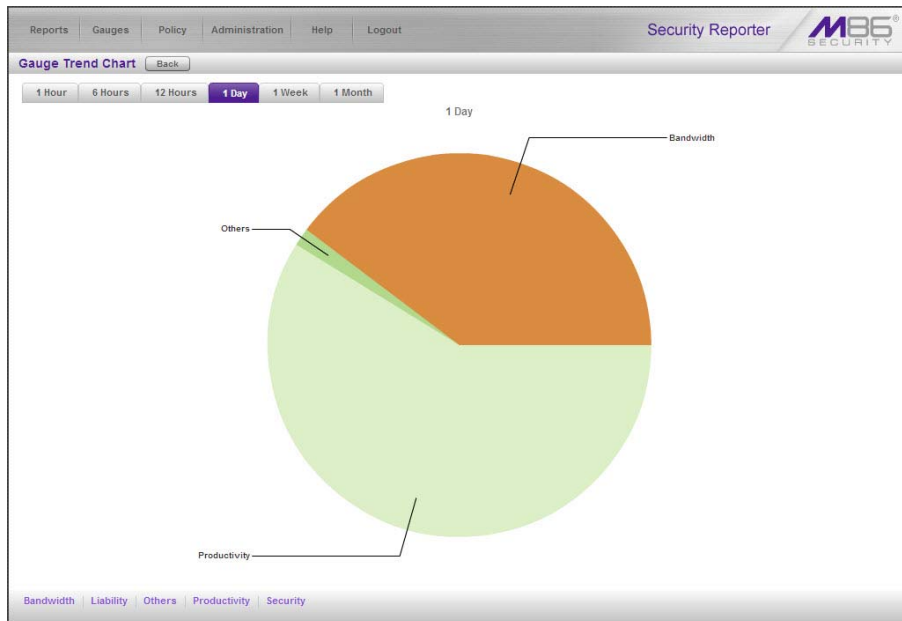
Now that you know how to access a pie trend chart showing overall gauge activity and how to drill down to view a line chart for a specific gauge, you will next learn how to access a pie chart for a specific gauge.

1. Go to the URL gauges Dashboard and click the middle icon at the bottom of the gauge:



2. The action of clicking the Trend Charts icon displays a pie Gauge Trend Chart for that gauge.

Figure 54: Gauge Trend Chart



Note the pie slices in this trend chart are named for each gauge component in which there was activity.

The time span represented in the trend chart can be changed by clicking one of five other tabs at the top of the chart.

Click a pie slice or tab beneath the pie chart to drill down into that gauge component and view a line chart showing that gauge component's activity within the specified time period.

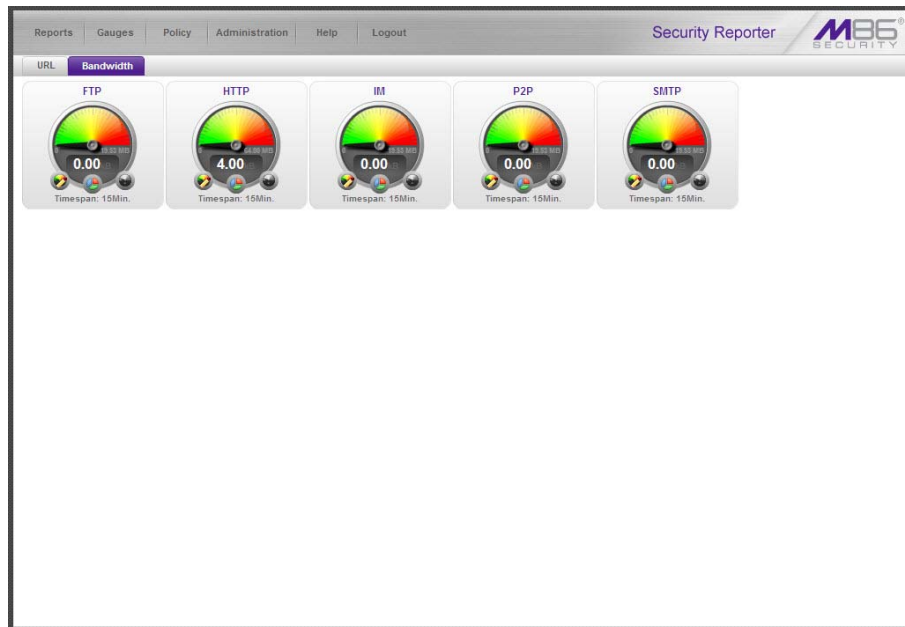
3.2.3 Monitor Bandwidth gauges

Once you've seen how URL gauges help you monitor end user Internet traffic, you will probably want to explore the ways bandwidth gauges help you monitor inbound and outbound bandwidth usage on your network.

3.2.3.1 How to view the Bandwidth gauges Dashboard

The bandwidth gauges Dashboard gives you an overview of current end user bandwidth activity on your network. To display this panel, first select **Gauges** and then click the Bandwidth tab above the Dashboard.

Figure 55: Bandwidth gauges Dashboard



Default bandwidth gauges include the following protocol gauges: FTP, HTTP, IM, P2P and SMTP. Protocol gauges are comprised of ports. For example, the FTP protocol includes ports 20 and 21.

Note the score in the middle of each gauge. This score shows the amount of bandwidth traffic in bytes (kB, MB, GB).

As with URL gauges, from this panel you can drill down to view end user activity in a bandwidth gauge and view trend charts on bandwidth gauge activity.

3.2.3.2 How to drill down into a Bandwidth gauge

Looking at the bandwidth gauges Dashboard, you can see at a glance which bandwidth gauge has the highest score. To identify the end users affecting that gauge, you will need to drill down into that gauge.

3.2.3.2.1 View Bandwidth protocol traffic information

In the bandwidth gauges Dashboard, click a high-scoring gauge to display the Gauge Ranking table showing all end user traffic for that protocol.

Figure 56: Bandwidth used by each end user for a protocol

Username	110	25	Total
192.168.20.77	0.00 kB	3.00 kB	3.00 kB

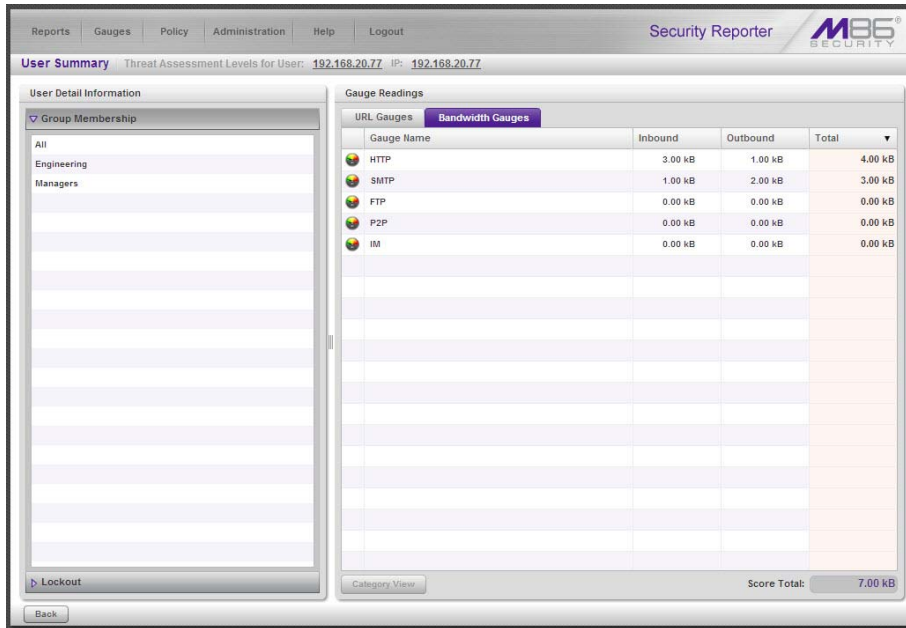
To the right of the User Name column are port numbers that comprise the protocol. The number of bytes of bandwidth used by each user displays in these columns.

3.2.3.2.2 View a user’s protocol usage information

To drill down and view a user’s bandwidth usage in all bandwidth gauge protocols, click a User Name to display the User Summary panel.

In the Gauge Readings sub-panel to the right side in this panel, click the Bandwidth Gauges tab to display each bandwidth Gauge Name and its corresponding Inbound, Outbound, and Total bytes of traffic used by that end user for that gauge:

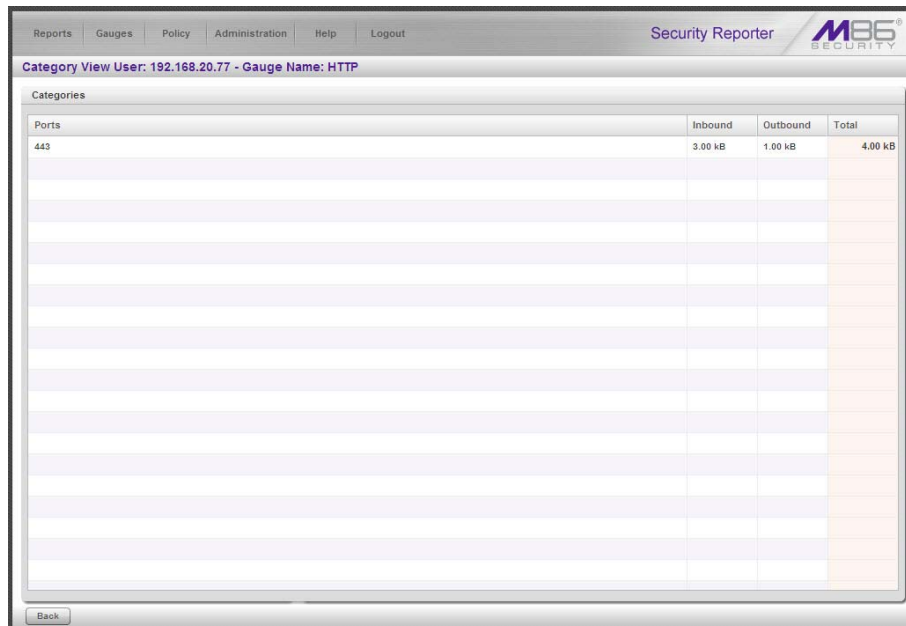
Figure 57: User Summary panel showing the user's bandwidth protocol usage



3.2.3.2.3 View a user's port usage information

Now drill down and view a user's port usage for a particular gauge. In the Gauge Readings sub-panel, click the Gauge Name to activate the **Category View** button. Click that button to display the Category View User panel.

Figure 58: Category View User panel showing the user's port usage



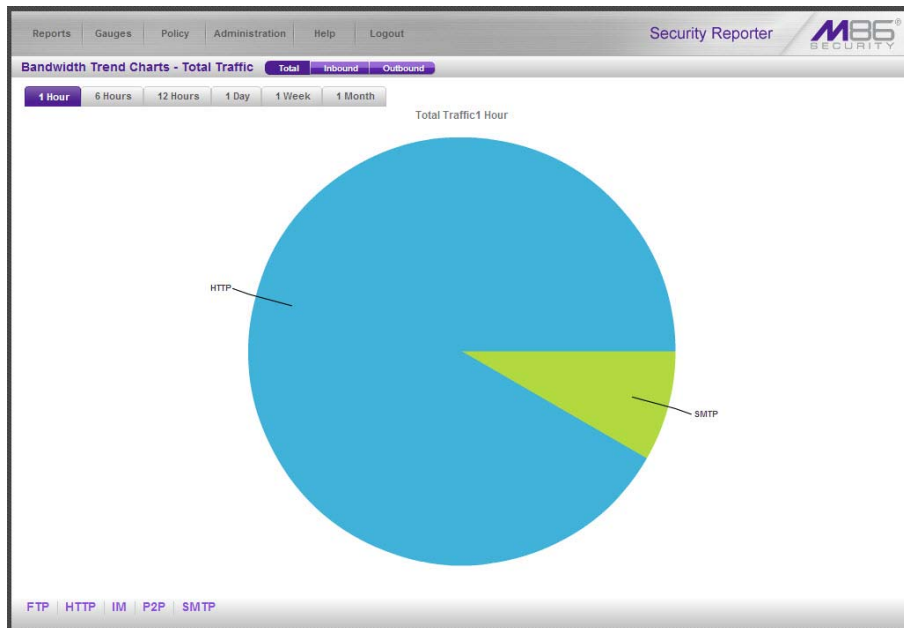
3.2.3.3 How to view Bandwidth Trend Chart activity

As you have seen with URL gauges, in addition to drilling down into a gauge to find out which end users are driving that gauge's activity, you can get an overall picture of a bandwidth gauge's current activity by generating a trend chart.

3.2.3.3.1 View overall activity in Bandwidth gauges

Navigate to Reports | Bandwidth Trend Charts to display the Bandwidth Trend Charts panel.

Figure 59: Bandwidth Trend Charts panel



The pie trend chart is divided into pie slices named for each bandwidth gauge in which there was activity. The size of each slice is determined by the amount of activity in that gauge for the designated time period, in comparison to activity in all other bandwidth gauges during that same time period. All activity is translated into a percentage figure, with the total activity for all slices equaling 100 percent.

You can change the time span represented in the trend chart by clicking one of five other tabs at the top of the chart. Choices range from the last hour to the last month of data.

3.2.3.3.2 View a line chart for a single Bandwidth gauge

To learn more about the activity for a particular gauge, click the pie slice for that gauge to view a line chart depicting that gauge's activity within the specified time period:



Note: The "score" on bandwidth gauges is based on the number bytes of bandwidth consumed; not page hits, as with URL gauges.

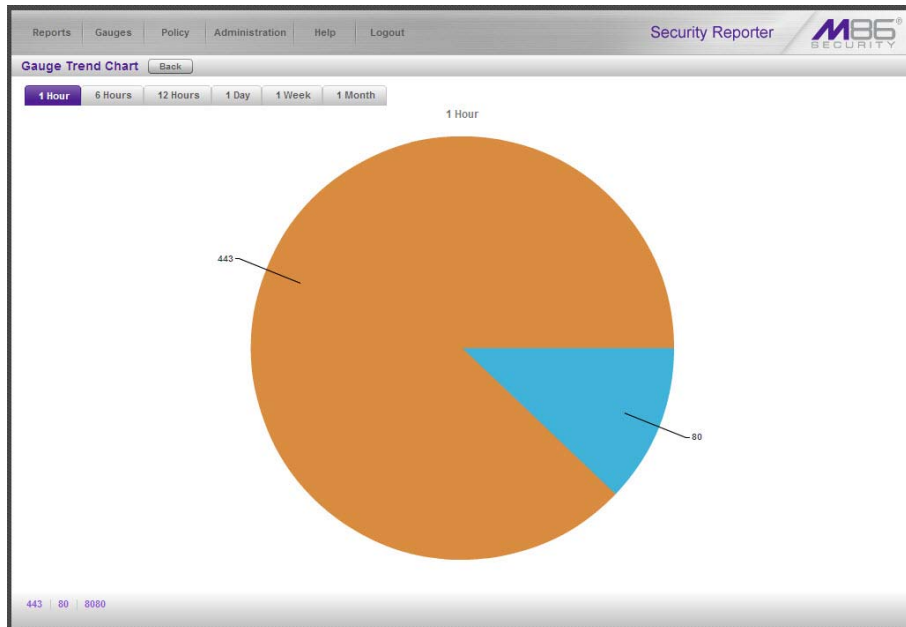
Figure 60: Line chart for a bandwidth gauge



3.2.3.4 How to view charts for a specific Bandwidth gauge

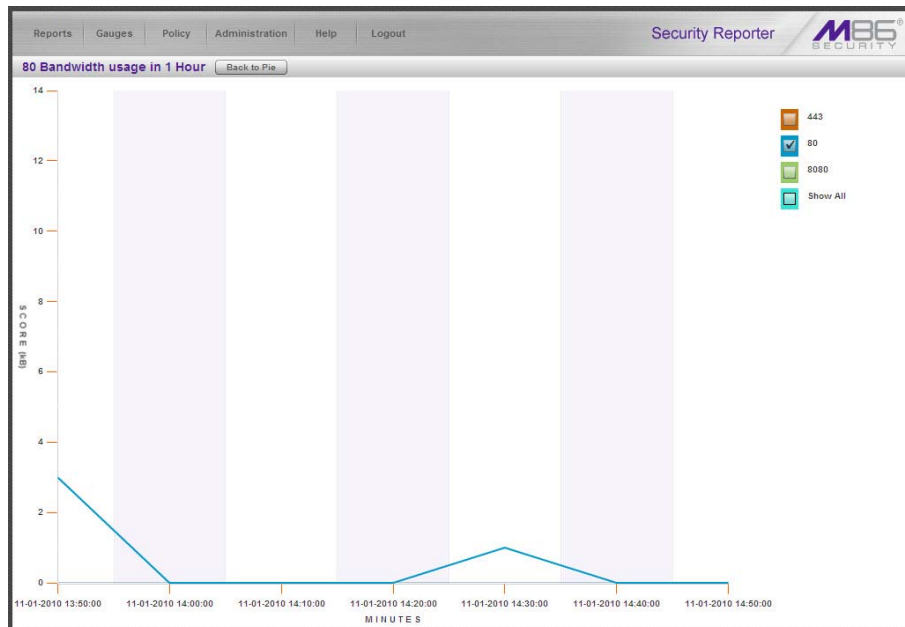
In the bandwidth gauges Dashboard, click the Trend Charts icon in the bottom middle of the gauge to display a pie trend chart for that gauge.

Figure 61: Bandwidth Gauge Trend Chart for a specified protocol (HTTP)



Click the pie slice or tab below to view a line chart showing traffic for that port.

Figure 62: Line chart for a specified port



3.2.4 Get the complete picture

As you have seen so far, the real time reporting section of the SR user interface lets you monitor URL and bandwidth gauge activity on your network. Analyzing data from both sources will give you a complete picture of the user's Internet usage behavior.

3.2.4.1 How to view Overall Ranking of user activity

The first step in finding out which end users are most actively driving gauges is to consult the Overall Ranking table that shows you a list of users affecting URL gauges and Bandwidth gauges, all in one panel. This ranking table is accessed by navigating to Gauges | Overall Ranking.

Figure 63: Overall Ranking table

The screenshot shows the Security Reporter interface with the 'Overall Ranking' section. It features two sub-panels: 'URL' and 'Bandwidth'. The 'URL' panel lists usernames and their scores, while the 'Bandwidth' panel lists usernames and their inbound/outbound traffic. The interface includes navigation tabs at the top and 'Previous'/'Next' buttons at the bottom of each table.

URL		Bandwidth		
Username	Score	Username	Inbound	Outbound
192.168.200.201	2967	192.168.168.71	5.54 MB	586 kB
192.168.200.45	1015	192.168.200.169	590 kB	176 kB
192.168.30.170	883	192.168.200.31	679 kB	80 kB
192.168.30.177	507	192.168.41.1	349 kB	71 kB
192.168.30.33	221	192.168.30.85	261 kB	16 kB
192.168.20.204	185	192.168.200.208	147 kB	102 kB
192.168.200.31	166	192.168.30.86	149 kB	51 kB
192.168.41.1	104	192.168.20.143	81 kB	21 kB
192.168.30.85	34	192.168.30.80	74 kB	16 kB
192.168.200.208	14	192.168.200.86	56 kB	22 kB
192.168.30.86	10	192.168.200.225	10 kB	65 kB
192.168.20.143	9	192.168.30.84	56 kB	17 kB
192.168.30.80	8	192.168.200.95	19 kB	40 kB
192.168.200.86	7	192.168.200.30	48 kB	9 kB
192.168.200.225	4	192.168.200.131	32 kB	18 kB
192.168.30.84	1	192.168.44.12	38 kB	7 kB
		192.168.30.87	14 kB	4 kB
		192.168.20.170	1 kB	16 kB
		192.168.200.201	10 kB	6 kB
		192.168.200.45	9 kB	5 kB
		192.168.30.170	11 kB	3 kB
		192.168.20.177	8 kB	6 kB
		192.168.30.33	6 kB	1 kB
		192.168.20.204	6 kB	1 kB
		192.168.20.213	5 kB	1 kB

Note the URL sub-panel to the left includes the User Name and Score of each user with activity in one or more URL gauges. The Bandwidth sub-panel to the right includes the User Name and number of bytes of Inbound and Outbound traffic used by that end user in one or more bandwidth gauges. Users listed in each sub-panel are ranked in order by their scores.

Clicking a Username link takes you to the User Summary panel where more details about that end user’s activity can be viewed, and action can be taken to restrict or prevent that end user’s Internet/network activities.

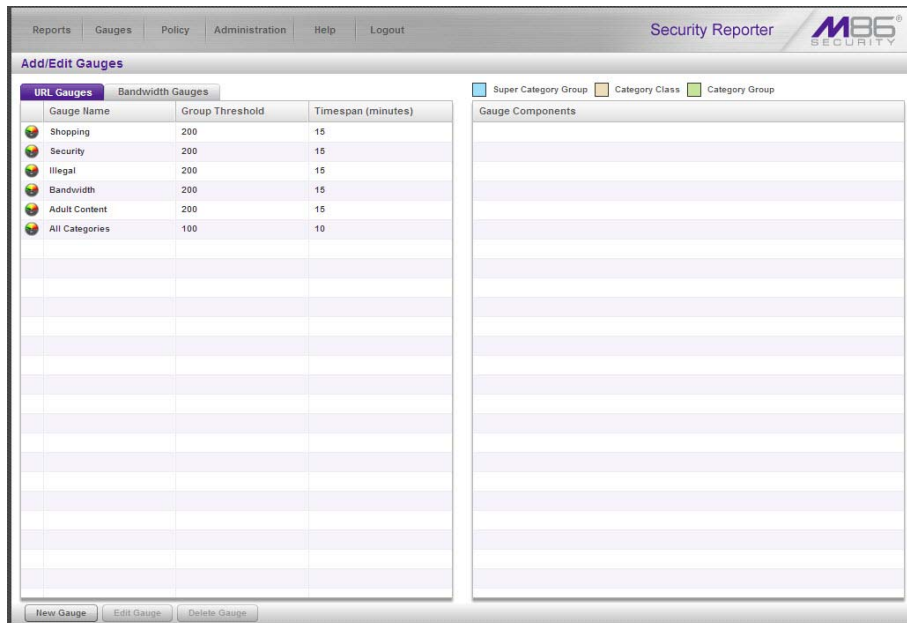
3.2.4.2 How to create a New Gauge

After working with the URL and bandwidth gauges for awhile, you may want to customize the default gauges or create your own to more effectively monitor the type of traffic on your network.

3.2.4.2.1 Select Add/Edit Gauges

In order to create a new custom gauge, navigate to Gauges | Add/Edit Gauges to display the panel by that name.

Figure 64: Add/Edit Gauges panel



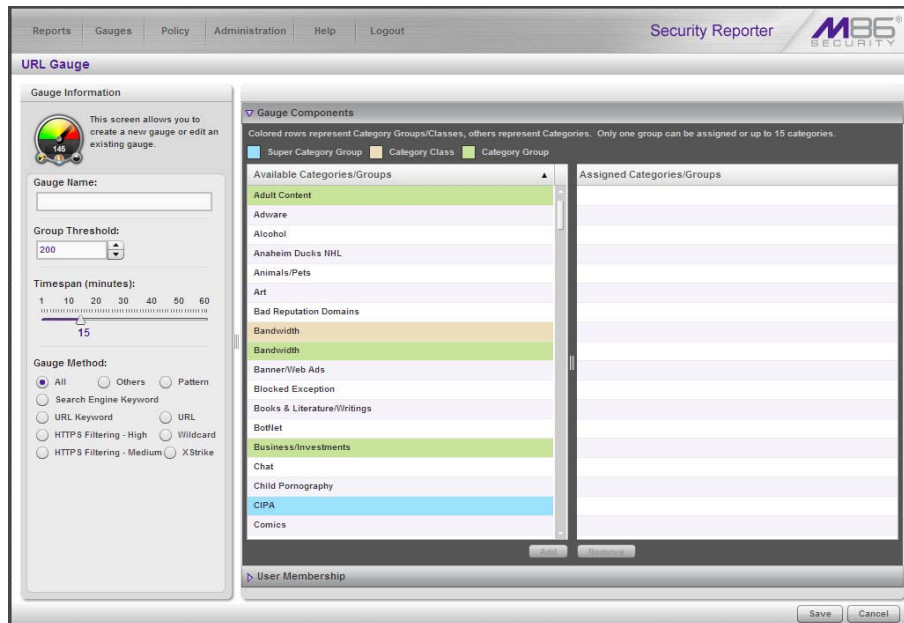
By default the URL Gauges tab displays, showing the list of URL gauges in the sub-panel to the left. If you wish to create a bandwidth gauge, click the Bandwidth Gauges tab to display the list of bandwidth gauges in this sub-panel.

Note that only five bandwidth gauges can be used at a time. If you wish to create a bandwidth gauge, an existing bandwidth gauge must first be deleted.

3.2.4.2.2 Add a New Gauge

Click the **New Gauge** button to display the URL Gauge or Bandwidth Gauge panel, as appropriate to the selection made in the previous panel.

Figure 65: URL Gauge panel

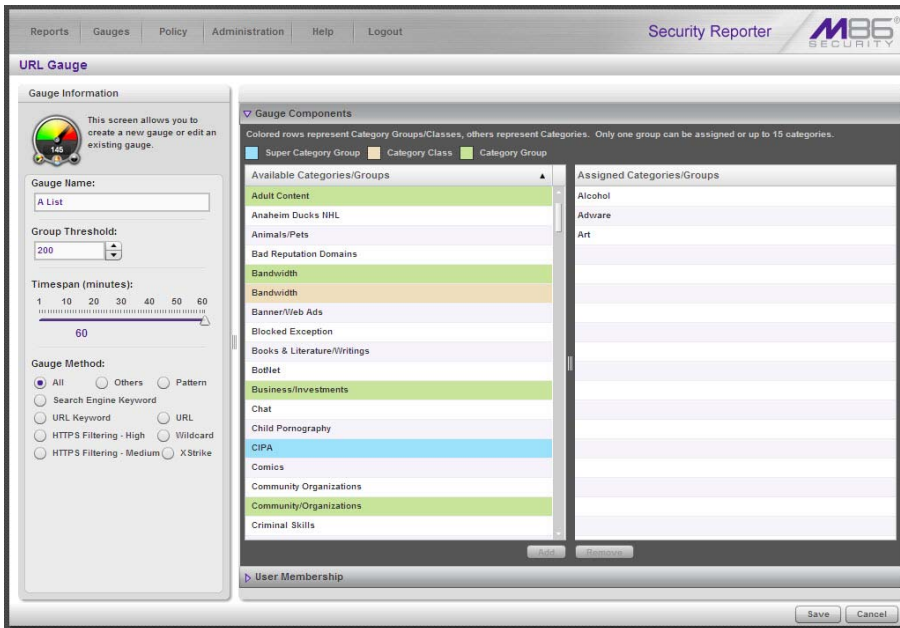


3.2.4.2.3 Specify Gauge Information

Set parameters for the custom gauge by making the following entries/selections in the Gauge Information sub-panel at the left side of the panel:

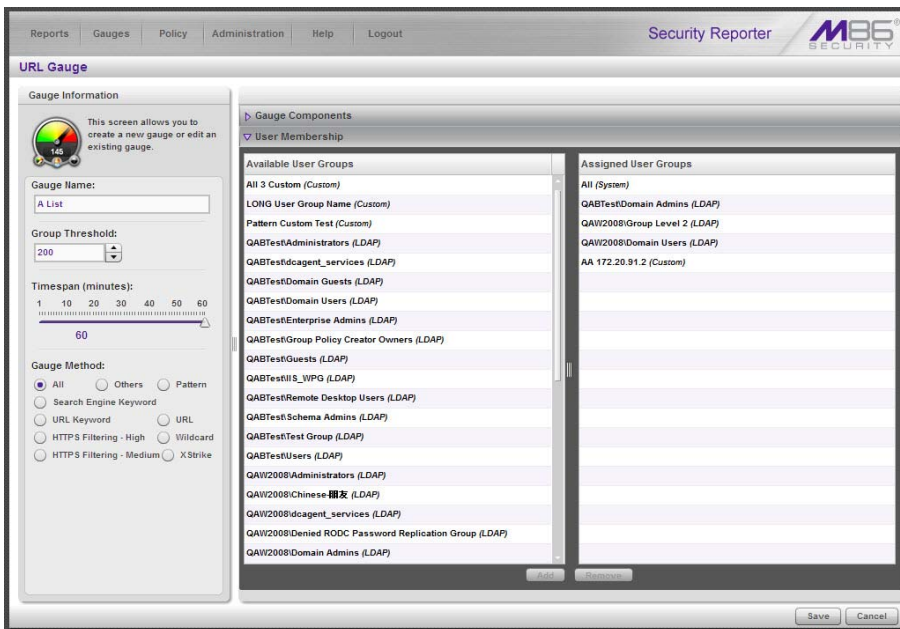
In the URL Gauge panel, do the following:

1. Type in a name in the **Gauge Name** field.
2. Leave the **Group Threshold** value at '200'.
3. Set a **Timespan** of '60' minutes by moving the slider tool to the right.
4. Leave the **Gauge Method** as 'All'.
5. In the Gauge Components accordion at the right side of the panel, go to the Available Categories/Groups box and move the "Adware", "Alcohol" and "Art" selections into the Available Categories/Groups list box by selecting each category and then clicking the **Add** button.



3.2.4.2.4 Select users to be monitored by the gauge

1. Click the User Membership accordion (located beneath the Gauge Components accordion) to open it:



2. From the Available User Groups box, choose the user groups whose activity will be monitored by this gauge, and then click the **Add** button.

3.2.4.2.5 Save gauge settings

Once you click **Save**, the Add/Edit Gauges panel redisplay and includes the Gauge Name of the gauge you just added. Your new gauge is now ready to show traffic.



Note: The initial gauge setup may take a few minutes. Once setup is complete, the gauge will report data in real time.

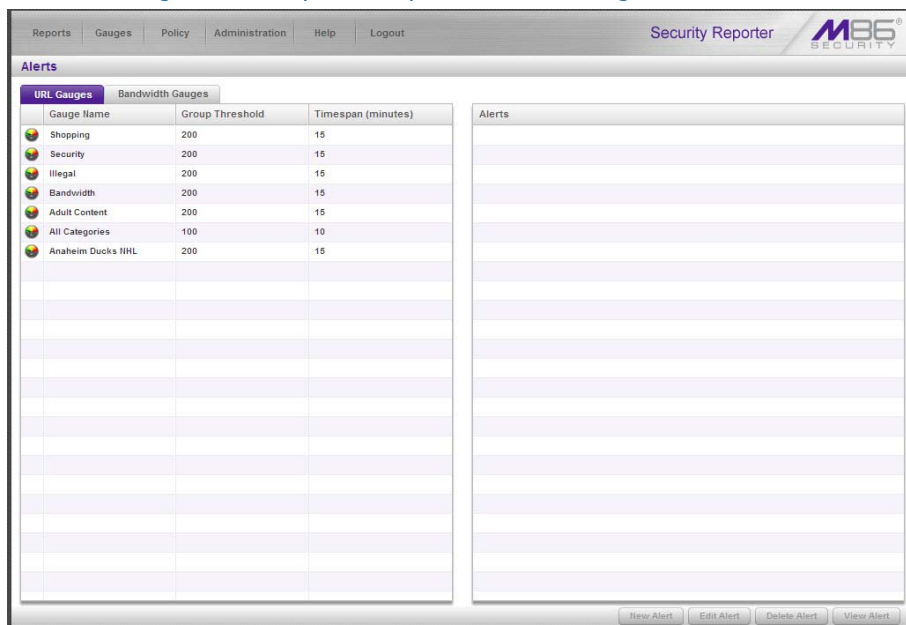
3.2.4.3 How to create an automated gauge alert

This section will step you through the process of creating an automated threshold per user, so you can be automatically notified via email and the violating user will be automatically locked out once a threshold is exceeded.

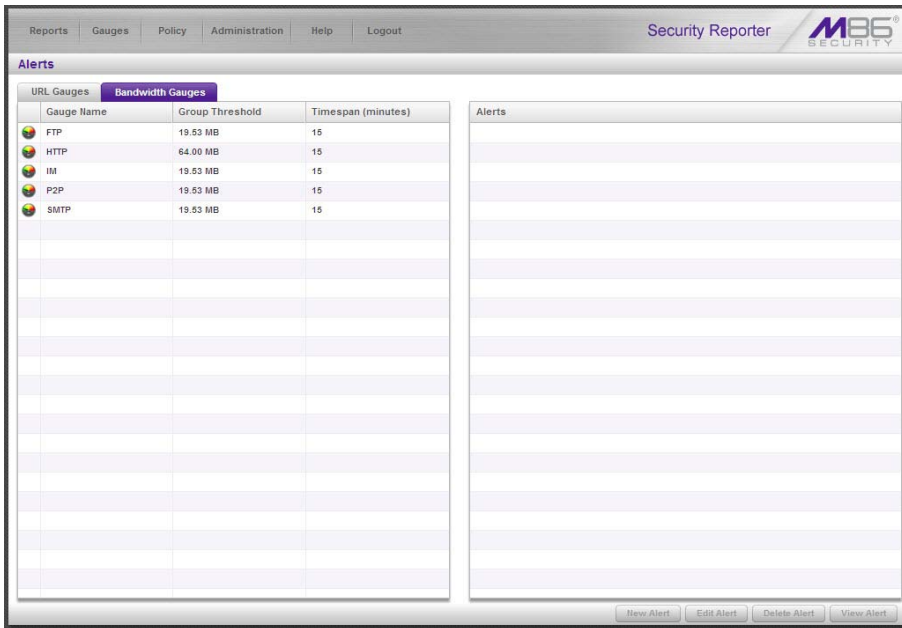
3.2.4.3.1 Set up a new alert

1. Navigate to Policy | Alerts to display the panel by the same name.

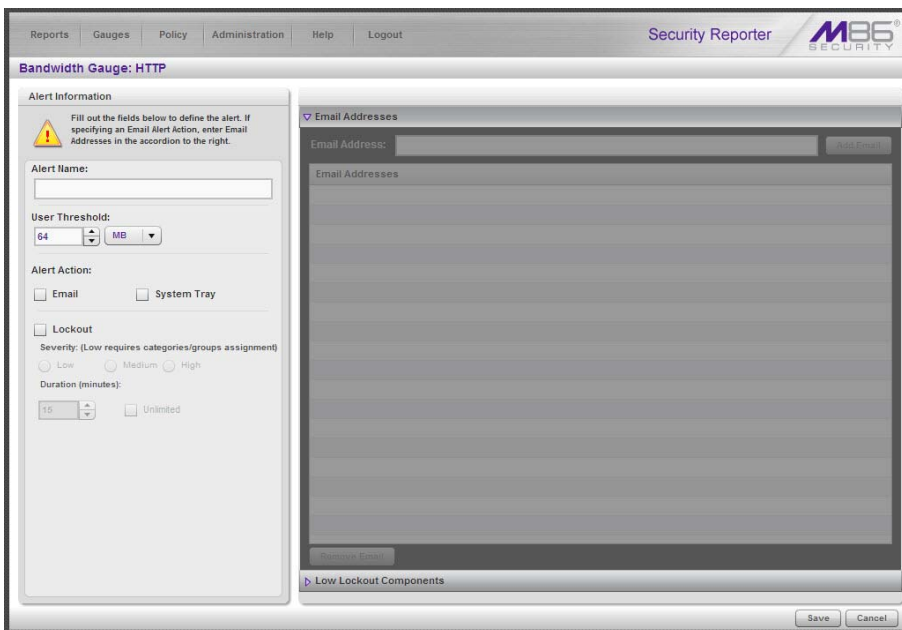
Figure 66: Sample Alerts panel with URL Gauges tab selected



2. By default the URL Gauges tab displays, showing all gauges currently in use. To create an alert for bandwidth gauges, click the Bandwidth Gauges tab:



3. Choose the Gauge Name from the list in the left side of the panel, and then click **New Alert** to display the next panel where you set parameters for the alert:



3.2.4.3.2 Specify Alert Information

Set parameters for the alert by making the following entries/selections in the Alert Information sub-panel at the left side of the panel:

1. Type in a name in the **Alert Name** field.
2. Specify the **User Threshold** value. This numeric value is the number of times each user will be allowed to visit categories monitored by the gauge before triggering an alert.

3. Enable **Alert Action** check boxes for "Email" and "Lockout."
4. Select a **Severity** level ("Low", "Medium", or "High"). This section is only enabled when the Lockout check box is selected.
 - For a URL gauge, a "Low" selection will lock out the user by the categories monitored by the specified URL gauge only. For a bandwidth gauge, a "Low" selection will lock out the user by the protocols or ports monitored by the specified bandwidth gauge.
 - A "Medium" selection will lock out the user from Internet access altogether.
 - A "High" selection will lock out the users from all network protocols, so they cannot access the Internet, send e-mails, use instant messaging, or use P2P or FTP.



Note: Time-based lockouts can be set for a range of 30 minutes, one hour to eight hours, or unlimited.

System Tray will not be shown in this demo, but if this feature is enabled, the administrator with an LDAP username, password and domain will see a system tray alert in the desktop system tray when an alert has been triggered. This applies to Active Directory environments only.

3.2.4.3.3 Specify criteria in the right side of the panel

If the Email Addresses accordion is closed, click to open it. Type in an **Email Address** and click the **Add Email** button. This is the address of the person who will be notified when an alert is triggered. You can add multiple email addresses.

Figure 67: Sample Bandwidth Gauges panel, email criteria

Security Reporter M36[®] SECURITY

Reports Gauges Policy Administration Help Logout

URL Gauge: Ducks NHL

Alert Information

Fill out the fields below to define the alert. If specifying an Email Alert Action, enter Email Addresses in the accordion to the right.

Alert Name:

User Threshold: 200

Alert Action: Email System Tray

Lockout

Severity: (Low requires categories/groups assignment)

Low Medium High

Duration (minutes): 15 Unlimited

Email Addresses

Email Address: Add Email

Email Addresses

Remove Email

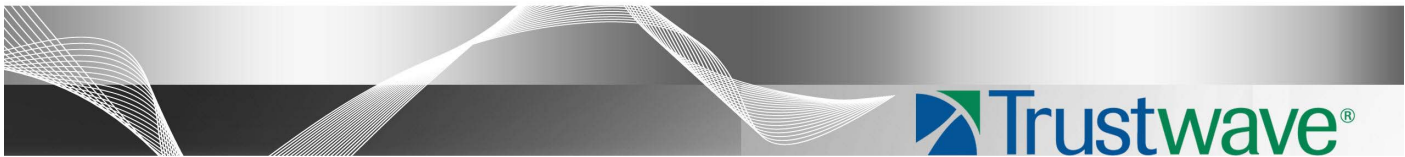
Low Lockout Components

Save Cancel

For a URL gauge alert, if a "Low" Lockout was specified, click the Low Lockout Components accordion to open it. Go to the Available Categories/Groups list box and move your selection(s) into the Assigned Categories/Groups list box by selecting each category and then clicking the **add >** button.

3.2.4.3.4 Save the alert

Click **Save** to save your settings and to display the Alerts panel with the new alert added.



About Trustwave®

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit <https://www.trustwave.com>.